รายงานการวิจัยเรื่อง

การพัฒนาเกณฑ์การประเมินมาตรการทางด้านการรักษาความปลอดภัย สำหรับหน่วยงานภาคเอกชน

Development of Security Measures Assessment for Private Organizations

โดย

ชัยเสฏฐ์ พรหมศรี

สุจิรา ไชยกุสินธุ์

วรัญญา แก้วเชือกหนัง

งานวิจัยเรื่องนี้ได้รับทุนสนับสนุนจากคณะบริหารธุรกิจ มหาวิทยาลัยเทคโนโลยีราชมงคลพระนคร

ประจำปีงบประมาณ พ.ศ. 2560

บทคัดย่อ

การศึกษานี้มีวัตถุประสงค์เพื่อกำหนดมาตรการทางด้านการรักษาความปลอดภัยให้สอดคล้องกับแนวปฏิบัติงานของหน่วยงานภาคเอกชน โดยดำเนินการวิจัยด้วยการวิเคราะห์เอกสาร (Documentary Analysis) และการทำสนทนากลุ่ม (Focus Group) โดยทำการสนทนากลุ่ม 1 ครั้งจากบุคคลที่เป็นตัวแทนด้านงานรักษาความปลอดภัยและมีประสบการณ์ด้านการจัดการงานรักษาความปลอดภัย จำนวน 8 คน และทำการสังเคราะห์และวิเคราะห์ข้อมูลที่ได้จากวิธีการทั้งสองมาบูรณาการเข้าด้วยกันเพื่อนำไปสู่การพัฒนาเกณฑ์เพื่อกำหนดมาตรการด้านการรักษาความปลอดภัย ซึ่งได้ผลการวิจัยประกอบไปด้วย การสร้างความตระหนักรู้เกี่ยวกับการพัฒนาด้านเทคโนโลยีที่เกี่ยวข้องกับการรักษาความปลอดภัย การบูรณการองค์ประกอบด้านสถาปัตยกรรม การพัฒนาระบบการรักษาความปลอดภัย การจัดการทรัพยากรมนุษย์ที่ครอบคลุมเจ้าหน้าที่รักษาความปลอดภัยและการให้ความรู้ที่เกี่ยวข้องกับบุคลากรในองค์การ และการกำหนดหลักปฏิบัติด้านการรักษาความปลอดภัยที่สอดคล้องกับธรรมชาติและกายภาพขององค์การ

คำสำคัญ: มาตรการการรักษาความปลอดภัย การพัฒนาเกณฑ์การรักษาความปลอดภัย องค์การเอกชน

Abstract

The objective of this qualitative study was to develop and determine security measures for private organizations. Documentary analysis and focus group technique were used as a method for gathering data. Eight participants who had experiences in security management were participated in a focus group. Data from two sources were gathered and integrated for data analysis. The results of data analysis led to the development of security measures factors. Findings indicated that there were five factors of security measures that needed to be implemented and carried out in private organizations including building awareness of technology development in security; integration of architectural security components; developing security systems; human resource management which encompasses security personnel and sharing knowledge; and determining appropriate security procedures that relate to nature and physical of organizations.

Keywords: Security measures, security measures development, private organizations

สารบัญ

บทที่ 1
บทนำ

1.1 ความสำคัญและที่มาของปัญหาที่ทำการวิจัย

ปัจจุบันองค์การทั้งภาครัฐและเอกชนส่วนใหญ่ให้ความสำคัญกับเรื่องมาตรการรักษาความปลอดภัยมากยิ่งขึ้น โดยครอบคลุมในเรื่อง บุคคล ข้อมูลข่าวสาร สถานที่ และการประชุมลับ ซึ่งปัจจัยที่สำคัญที่ส่งผลต่อการสร้างมาตรการรักษาความปลอดภัยให้เข้มแข็งและมีประสิทธิภาพและประสิทธิผลสูงสุด คือ การสร้างความตระหนักรู้ของบุคลากรในองค์การ ที่มีต่อความมั่นคงปลอดภัย ความรู้สึกถึงความไม่มั่นคงปลอดภัยต่อชีวิตและทรัพย์สินของบุคลากรในองค์การถือว่าเป็นอันตรายต่อการดำเนินองค์การไปสู่การบรรลุเป้าหมายเป็นอย่างมาก ดังนั้นการสร้างมาตรการเรื่องความมั่นคงปลอดภัยจึงเป็นสิ่งที่สำคัญสำหรับองค์การ ทั้งนี้เพราะความสามารถทางด้านการจัดการความมั่นคงปลอดภัยขององค์การช่วยให้ลูกค้าเกิดความเชื่อมั่นว่าองค์กรสามารถคุ้มครองดูแล ปกป้องทรัพย์สินและชีวิตของผู้ที่มาใช้บริการได้ ทำให้ผู้มีส่วนได้ส่วนเสียขององค์การเกิดความเชื่อมั่น ถ้าองค์การใดมีการจัดการความมั่นคงปลอดภัยที่มีประสิทธิภาพหรือสามารถลดความเสี่ยงทางด้านความมั่นคงปลอดภัยลงได้ องค์การนั้นก็มีโอกาสที่จะบรรลุเป้าหมายได้อย่างมีประสิทธิภาพและประสิทธิผล ในทางตรงกันข้ามหากองค์การใด ไม่สามารถจัดการความมั่นคงปลอดภัยได้อย่างมีประสิทธิภาพอาจส่งผลกระทบต่อการบริหารองค์การในระยะยาวได้ เพราะผู้มีส่วนได้ส่วนเสียขององค์การจะเกิดความรู้สึกไม่มั่นใจกับความมั่นคงปลอดภัยต่อชีวิตและทรัพย์สินอันมีค่าของตนซึ่งอาจทำให้หมดความไว้วางใจได้

อย่างไรก็ดี ถึงแม้ว่าการสร้างแนวทางในการรักษาความมั่นคงปลอดภัยจะมีความสำคัญสำหรับทุกองค์การ แต่จากการทบทวนวรรณกรรมที่เกี่ยวข้องพบว่า แต่ละหน่วยงานจะดำเนินการไปในลักษณะต่างฝ่ายต่างปฏิบัติ ไม่มีมาตรฐานกลางที่ชัดเจนที่จะกำหนดหรือใช้ในการประเมินเพื่อวัดคุณภาพของแนวทางในการรักษาความมั่นคงปลอดภัยในภาพรวม นอกเหนือจากระเบียบสำนักนายกรัฐมนตรีว่าด้วยการรักษาความปลอดภัยแห่งชาติ พ.ศ. 2552 ด้วยเหตุนี้การพัฒนาเกณฑ์การประเมินมาตรการทางด้านการรักษาความปลอดภัยเพื่อนำไปสู่การกำหนดแนวทางปฏิบัติร่วมกันในเบื้องต้นของหน่วยงานภาครัฐจึงเป็นสิ่งจำเป็นอย่างยิ่ง และสามารถนำไปเชื่อมโยงกับระดับความสำคัญและประเภทขององค์การที่แตกต่างกันเพื่อนำไปสู่การกำหนดมาตรการทางด้านการรักษาความปลอดภัยที่จะนำไปประยุกต์ได้อย่างมีประสิทธิภาพและประสิทธิผลสูงสุดในแต่ละองค์การ งานวิจัยนี้จึงมีวัตถุประสงค์เพื่อพัฒนาเกณฑ์การประเมินมาตรการทางด้านการรักษา

ความปลอดภัยสำหรับองค์การภาครัฐ ซึ่งถือเป็นหัวใจสำคัญของปฏิบัติการทางด้านการรักษาความปลอดภัยที่ทำให้เกิดประโยชน์สูงสุดต่อองค์การ

1.2 วัตถุประสงค์ของการวิจัย

1. เพื่อกำหนดมาตรการทางด้านการรักษาความปลอดภัยให้สอดคล้องกับแนวปฏิบัติงานของหน่วยงานภาคเอกชน

2. เพื่อพัฒนาเกณฑ์การประเมินมาตรการทางด้านการรักษาความปลอดภัยสำหรับองค์การภาคเอกชน

3. เพื่อสร้างกรอบมาตรฐานในการประเมินมาตรการทางด้านการรักษาความปลอดภัยในองค์การภาคเอกชน

1.3 ขอบเขตของโครงการวิจัย

ด้านเนื้อ ศึกษาแนวทางในการพัฒนาเกณฑ์การประเมินมาตรการทางด้านการรักษาความปลอดภัยสำหรับองค์การภาคเอกชน

ด้านประชากร กลุ่มตัวอย่างที่เกี่ยวข้องได้แก่ บริษัทด้านการรักษาความปลอดภัย

ด้านระยะเวลา ตุลาคม 2559 – กันยายัน 2560

1.4 คำถามที่เกี่ยวข้องสำหรับการวิจัย

1. อะไรคือมาตรการทางด้านการรักษาความปลอดภัยของหน่วยงานภาคเอกชน

2. อะไรคือเกณฑ์การประเมินมาตรการทางด้านการรักษาความปลอดภัยสำหรับองค์การภาคเอกชน

3. อะไรคือกรอบมาตรฐานในการประเมินมาตรการทางด้านการรักษาความปลอดภัยในองค์การภาคเอกชน

บทที่ 2
การทบทวนวรรณกรรม

2.1 แนวคิดที่เกี่ยวข้องกับการรักษาความปลอดภัยและความมั่นคงปลอดภัย

2.1.1 ความหมายของการรักษาความปลอดภัยและความมั่นคงปลอดภัย

ในระเบียบว่าด้วยการรักษาความปลอดภัยแห่งชาติ พ.ศ. 2517 ได้ให้คำจำกัดความของ “การรักษาความปลอดภัย” ว่าหมายถึง “บรรดามาตรการที่กำหนดขึ้น ตลอดจนการดำเนินการทั้งปวงเพื่อพิทักษ์รักษาและคุ้มครองป้องกันสิ่งที่เป็นความลับของทางราชการข้าราชการ ส่วนราชการและทรัพย์สินของแผ่นดินให้พ้นจากการรั่วไหล การจารกรรม การก่อวินาศกรรม การบ่อนทำลาย และการกระทำอื่นใดที่มีผลกระทบกระเทือน หรือเป็นภัยต่อความมั่นคงแห่งชาติ” (เว็บไซต์สำนักข่าวกรองแห่งชาติ, 2551)

เดช จรูญเรืองฤทธิ์ (2549, หน้า 70-72) ได้อธิบายคำว่า “การรักษาความปลอดภัย” หรือ “ความปลอดภัย” หรือ “ความมั่นคง” ว่ามีการแปลมาจากคำภาษาอังกฤษคำเดียวกันคือ “Security” และได้ถูกนำไปใช้ในหลายเรื่องหลายระดับ ทำให้มีความหมาย มีขอบเขตที่จะต้องมีการพิจารณาและ/หรือมีมาตรการที่จะนำไปใช้ในการปฏิบัติในรายละเอียดต่างๆ กันไปเฉพาะเรื่อง เฉพาะระดับ ซึ่งถ้าพิจารณาในระดับของธุรกิจเอกชน “การรักษาความปลอดภัย” มุ่งเน้นไปที่เรื่องการป้องกันภัย หรือป้องกันความเสียหายที่กระทบกระเทือนต่อผลประโยชน์ ต่อธุรกิจ ต่อองค์กร ของตน เช่น การทุจริตของพนักงาน การโจรกรรม การจารกรรม การก่อวินาศกรรม การบ่อนทำลาย อัคคิภัย และอุบัติเหตุที่ทำให้เสียหายต่างๆ

เคอร์ตัส (Kurtus, 2001) ได้ให้ความหมายของคำว่า “ความมั่นคงปลอดภัย (Security)” ว่าคือ การปกป้องบุคคล ทรัพย์สินหรือองค์กรจากการโจมตี ซึ่งการโจมตีแบ่งออกเป็น 3 ประเภท ได้แก่

1) การโจมตีบุคคล (Attack on person) เป็นความพยายามที่จะทำร้ายหรือเอาชีวิตบุคคลใดบุคคลหนึ่ง หรืออาจเป็นการโจมตีเพื่อที่จะให้บุคคลได้รับความบาดเจ็บหรือกระทบกระเทือนทางจิตใจ อารมณ์และสถานทางการเงิน และในบางครั้งการโจมตีประเภทนี้มุ่งที่จะทำลายชื่อเสียงของบุคคลที่เป็นเป้าหมายอีกด้วย

2) การโจมตีทรัพย์สิน (Attack on property) เป็นความพยายามที่จะทำลายหรือก่อให้เกิดความเสียหายต่อทรัพย์สิน เช่น อาคารบ้านเรือน หรือสิ่งของต่างๆ ขโมยหรือโจรเป็นตัวอย่างของกลุ่มบุคคลที่มุ่งโจมตีต่อทรัพย์สินของบุคคลอื่น

3) การโจมตีองค์กรหรือหน่วยงาน (Attack on organization) เป็นกลุ่มหรือบุคคลที่มุ่งหวังที่จะทำลายองค์กรใดองค์กรหนึ่งไม่ว่าจะเป็นภาครัฐหรือเอกชน ซึ่งการโจมตีเกี่ยวข้องกับ การก่อวินาศกรรม การทำลายชีวิตและทรัพย์สินของบุคคลในองค์กร รวมทั้งการเอาชีวิตผู้นำในองค์กรแห่งนั้นด้วย

จิตรเจริญ เวลาดี (2541 อ้างถึงใน ภาสกร สถิติยุทธการ, 2545, หน้า 6) กล่าวว่า การรักษาความปลอดภัย คือ การระวังดูแลป้องกันให้พ้นภัย หรือพ้นไปจากเหตุที่ทำให้เกิดความเสียหาย การรักษาความปลอดภัย หมายถึง การป้องกันบุคคล ข่าวสาร สถานที่และทรัพย์สิน ตลอดจนกิจการของหน่วยงานใดๆ ให้พ้นจากการกระทำใดๆ ที่มีผลกระทบกระเทือนต่อความมั่นคงปลอดภัย หรือประโยชน์ขององค์การนั้นๆ

ภาสกร สถิติยุทธการ (2545, หน้า 6-7) ได้สรุปว่า สาระสำคัญของการรักษาความปลอดภัย คือ การยับยั้ง ขัดขวางหรือป้องกันไว้ก่อนที่จะเกิดความเสียหาย และบรรเทาความเสียหายให้น้อยที่สุด ดังนั้นจึงต้องมีการดำเนินการอย่างเป็นระบบ โดยเชื่อมโยงระหว่างการรักษาความปลอดภัยเข้ากับการปฏิบัติงานตามปกติของหน่วยงาน

สรุป การรักษาความปลอดภัย คือ มาตรการที่กำหนดขึ้นเพื่อใช้ในการป้องกันหรือยับยั้งภยันตรายที่อาจก่อให้เกิดความเสียหายต่อบุคลากร ข่าวสาร สถานที่และทรัพย์สินขององค์การ

2.1.2 ภัยต่อความมั่นคงปลอดภัย

เดช จรูญเรืองฤทธิ์ (2549, หน้า 76-83) ได้ให้ความหมายของคำว่าภัย ว่าคือ “การกระทำ หรือ เหตุ หรือ สภาพ ที่ทำให้เกิดความเสียหาย” ซึ่งสามารถแบ่งออกได้เป็น 2 ประเภทใหญ่ ได้แก่

2.1.2.1 ภัยธรรมชาติ (Natural disasters) เช่น ภัยจากน้ำท่วม ฝนแล้ง ฟ้าผ่า แผ่นดินไหว ภูเขาไฟระเบิด เป็นต้น ภัยประเภทนี้ไม่มีคนหรือมาตรการใดป้องกัน หรือห้ามไม่ให้เกิดได้สามารถทำได้แค่เพียงการวางมาตรการบรรเทาความเสียหายเมื่อเกิดขึ้นแล้วเท่านั้น

2.1.2.2 ภัยจากกระทำของคน (Human acts) ซึ่งแบ่งย่อยออกเป็น 2 ประเภท คือ

1) ภัยจากกระทำของคนโดยไม่เจตนาหรือไม่ตั้งใจ (Accidental acts) ซึ่งส่วนมากจะเกิดจากการประมาทเลินเล่อ รู้เท่าไม่ถึงการณ์ ของคนทำที่ก่อให้เกิดอุบัติเหตุ ซึ่งภัยประเภทนี้มีลักษณะกระทำโดยเปิดเผย และไม่ตั้งใจ เช่น ทิ้งก้นบุหรี่ในถังขยะทำให้เกิดเพลิงไหม้ หรือเสียบปลั๊กไว้แล้วเกิดไฟฟ้าลัดวงจรทำให้เกิดเพลิงไหม้ขึ้น การป้องกันภัยประเภทนี้เรียกว่า “การป้องกันอุบัติเหตุ (safety)” ซึ่งดำเนินการได้โดยการวางแผน วางระเบียบปฏิบัติงาน และวางมาตรการในการควบคุมและฝึกอบรมคนไม่ให้ประมาท

2) ภัยจากการกระทำของคนโดยเจตนาหรือตั้งใจ (Criminal acts) ภัยประเภทนี้ผู้กระทำมักตั้งใจทำและปกปิดการกระทำของตนเพราะจะมีความผิดทางอาญา ภัยประเภทนี้เป็นภัยสำคัญที่คุกคามองค์กรและหน่วยงานต่างๆ ในปัจจุบัน การป้องกันภัยนี้จะเรียกว่า “การรักษาความปลอดภัย (security)”

เดมกิน (Demkin, 2003, หน้า 21-23) กล่าวว่าภัยคุกคามที่สามารถทำลายหรือเป็นอันตรายต่อทรัพย์สินและองค์กรได้ แบ่งออกเป็น 2 ประเภท ได้แก่

1) ภัยคุกคามที่เกิดขึ้นโดยสาเหตุทางธรรมชาติ ซึ่งเรียกว่า “ภัยคุกคามทางด้านความปลอดภัย (Safety threats)” ซึ่งภัยประเภทนี้เป็นภัยที่เกิดขึ้นโดยไม่ตั้งใจ เพราะเป็นเหตุมาจากปรากฏการณ์ทางธรรมชาติ เช่น ฟ้าผ่า ฟ้าร้อง น้ำท่วม พายุต่างๆ หรือมาจากความเลินเล่อหรือประมาทของมนุษย์ เช่น การใช้วัตถุบางชนิดอย่างไม่เหมาะสม อุบัติเหตุ หรือความผิดพลาดของเครื่องมือ ระบบและอุปกรณ์

2) ภัยที่เกิดขึ้นจากน้ำมือของมนุษย์ ซึ่งเรียกว่า “ภัยคุกคามทางด้านความมั่นคงปลอดภัย (Security threats)” ซึ่งภัยประเภทนี้เกิดขึ้นโดยความตั้งใจหรือจากการกระทำของมนุษย์ ซึ่งการกระทำนั้นอาจมาจากบุคคลที่มีอารมณ์ฉุนเฉียวรุนแรง หรือจากอาชญากร หรือจากผู้ก่อการร้ายก็ได้ ซึ่งแนวทางในการสร้างภัยคุกคามทางด้านความมั่นคงปลอดภัย ได้แก่ การโจมตีโดยอาวุธ (Ballistic attacks) การใช้ระเบิด (Bombs) การโจมตีโดยสารเคมี (Chemical) หรือสารชีวภาพ (Biological) หรือรังสีต่างๆ (Radiological) หรือรวมกันเรียกว่า CBR contamination และการโจมตีทางคอมพิวเตอร์ (Cybercrime)

2.2 มาตรการในการรักษาความปลอดภัย

การรักษาความปลอดภัยวัตถุประสงค์หลักของการรักษาความปลอดภัยหรือการวางมาตรการรักษาความปลอดภัยมีด้วยกัน 2 ประการ ได้แก่ (เดช จรูญเรืองฤทธิ์, 2549, หน้า 200)

2.2.1 ลดโอกาสที่จะเกิดภัยหรือลดการเสี่ยงภัยให้เหลือน้อยที่สุด

2.2.2 บรรเทาความเสียหาย หากภัยเกิดขึ้น

ซึ่งมาตรการในการรักษาความปลอดภัย ซึ่งถือเป็นเครื่องมือที่จะนำไปใช้ในการปฏิบัติเพื่อบรรลุวัตถุประสงค์ 2 ประการของการรักษาความปลอดภัย ประกอบด้วย 3 ประเภท คือ

1) การรักษาความปลอดภัยเกี่ยวกับบุคคล (Personal security) คือ “มาตรการที่กำหนดขึ้นสำหรับใช้ปฏิบัติต่อข้าราชการ หรือผู้ที่ได้รับความไว้วางใจให้เข้าถึงสิ่งที่เป็นความลับของทางราชการ หรือให้ปฏิบัติหน้าที่ราชการที่สำคัญเพื่อให้เป็นที่เชื่อแน่ว่าต้องเป็นผู้ที่ไม่เป็นภัยต่อความมั่นคงของประเทศชาติ” (เดช จรูญเรืองฤทธิ์, 2549, หน้า 216)

2) การรักษาความปลอดภัยเกี่ยวกับเอกสาร (Documental security) คือ “มาตรการที่กำหนดขึ้นสำหรับปฏิบัติต่อเอกสารลับ เพื่อป้องกันไม่ให้ผู้ไม่มีอำนาจหน้าที่ได้ล่วงรู้ หรือเข้าถึงเอกสารนั้น” (เดช จรูญเรืองฤทธิ์, 2549, หน้า 248)

3) การรักษาความปลอดภัยเกี่ยวกับสถานที่ (Physical security) คือ “มาตรการที่กำหนดขึ้นเพื่อพิทักษ์รักษาให้ความปลอดภัยที่สงวน อาคาร และสถานที่ของส่วนราชการ ตลอดจนวัสดุอุปกรณ์ เจ้าหน้าที่และเอกสารในอาคารสถานที่ดังกล่าวให้พ้นจากการโจรกรรม การจารกรรม และการก่อวินาศกรรม หรือเหตุอื่นใดอันอาจจะทำให้เสียสมรรถภาพในการปฏิบัติภารกิจของส่วนราชการได้” ซึ่งถ้ากล่าวโดยสรุปโดยไม่เน้นที่ส่วนราชการแต่เพียงอย่างเดียว การรักษาความปลอดภัยสถานที่ คือ การป้องกันอาคาร สถานที่ ทรัพย์สิน ตลอดจนบุคคลในสถานที่ให้พ้นจากภัย (เดช จรูญเรืองฤทธิ์, 2549, หน้า 313)

การรักษาความปลอดภัยสถานที่มีจุดมุ่งหมายด้วยกัน 4 ประการ ได้แก่ (เว็บไซต์กรมพินิจและคุ้มครองเด็กและเยาวชน, 2551)

1) กำหนดมาตรฐานการรักษาความปลอดภัยเกี่ยวกับสถานที่ของหน่วยงานหรือองค์กรนั้น

2) เป็นแนวทางในการวางแผนรักษาความปลอดภัยเกี่ยวกับสถานที่ตั้งขึ้นใหม่หรือขยายออกไป และเป็นแนวทางในการประเมินค่าแห่งการรักษา ความปลอดภัยเกี่ยวกับสถานที่ที่มีอยู่แล้ว

3) เป็นแนวทางให้ส่วนราชการดำเนินมาตรการรักษาความปลอดภัยเกี่ยวกับสถานที่ตามความเหมาะสมกับระดับความสำคัญของสถานที่นั้นๆ

4) ช่วยเจ้าหน้าที่รับผิดชอบในการพิทักษ์รักษาสถานที่และวัตถุต่างๆ ที่มีค่าสำหรับองค์กรให้ปฏิบัติงานได้อย่างมีประสิทธิภาพ

การรักษาความปลอดภัยสถานที่ที่มีประสิทธิภาพ ต้องเป็นการป้องกันร่วมกันระหว่าง “คน” และ “วัตถุ” โดยหลักการแล้ว “คน” มีความสำคัญมากกว่า “วัตถุ” เพราะ “คน” เป็นผู้ที่ทำให้ระบบหรือมาตรการรักษาความปลอดภัยมีความเข้มแข็งและเกิดผลในทางปฏิบัติได้มากที่สุด (เดช จรูญเรืองฤทธิ์, 2549, หน้า 316) ซึ่งคนมีหน้าที่ 3 ประการในการรักษาความปลอดภัยเกี่ยวกับสถานที่ ได้แก่

1) คอยเฝ้าตรวจ (Detection) คือ การตรวจตราผู้ที่ผ่านเข้ามาในสถานที่ทุกคน

2) พิสูจน์ทราบ (Identification) คือ ระบุว่าบุคคลที่กำลังจะเข้ามาในสถานที่นั้นเป็นผู้ที่มีสิทธิหรือไม่หรือเป็นผู้ไม่พึงประสงค์หรือไม่

3) สกัดกั้นหรือขัดขวาง (Interception) คือ การกระทำหลังจากทำการพิสูจน์ทราบแล้วว่าผู้ที่ผ่านเข้ามาเป็นผู้ที่ไม่มีสิทธิ หรือเป็นผู้ที่ไม่พึงประสงค์ ก็ทำการสกัด ขัดขวาง จับกุมตามสมควรแก่กรณี

นอกจากนี้ เดช จรูญเรืองฤทธิ์ (2549, หน้า 324-325) ยังได้อธิบายว่า องค์กรต้องให้ความสำคัญกับมาตรการรักษาความปลอดภัยเกี่ยวกับสถานที่ โดยพิจารณารายละเอียดหรือส่วนประกอบต่างๆ ดังต่อไปนี้

1) ต้องจัดให้มีพื้นที่การรักษาความปลอดภัย (Restricted area) หมายถึง พื้นที่หรือบริเวณใดขององค์กรที่มีการกำหนดขอบเขตโดยแน่ชัด มีข้อจำกัดและการควบคุมการเข้าออกเป็นพิเศษตามความสำคัญของแต่ละพื้นที่ โดยมีจุดมุ่งหมายเพื่อจะรักษาบุคคล ทรัพย์สิน หรือวัสดุอุปกรณ์ที่สำคัญของหน่วยงานให้ปลอดภัย ซึ่งโดยทั่วไปอาจมีการแบ่งพื้นที่ตามความสำคัญ เช่น พื้นที่ควบคุม (Controlled area) ซึ่งเป็นพื้นที่ที่อยู่ในขอบเขตของพื้นที่ที่มีการรักษาความปลอดภัย โดยการผ่านเข้าออกพื้นที่ต้องมีระเบียบการควบคุมบุคคลและยานพาหนะเพื่อช่วยในการกลั่นกรองในเบื้องต้น และพื้นที่หวงห้าม (Limited area) ซึ่งเป็นพื้นที่ที่มีการรักษาความปลอดภัยสิ่งที่เป็นความลับชั้นต่างๆ ตลอดจนบุคคลสำคัญ ทรัพย์สิน หรือวัสดุอุปกรณ์สำคัญของหน่วยงาน

2) ต้องมีการระวังป้องกันทางวัตถุ (Physical protection) หมายถึง การนำเอาวัตถุมาสร้างเป็นเครื่องกีดขวางเพื่อแสดงขอบเขตของสถานที่ หรือพื้นที่บริเวณใดบริเวณหนึ่ง และ/หรือ เพื่อทำหน้าที่จำกัดหรือขัดขวางการเข้าไปสู่สถานที่หรือพื้นที่นั้น หรือหน่วงเหนี่ยวการล่วงล้ำเพื่อให้ยามรักษาการณ์มีโอกาสตรวจพบ หยุดยั้ง หรือจับกุมได้ อีกทั้งเป็นการประหยัดจำนวน เจ้าหน้าที่ยามรักษาการณ์ และเป็นการบังคับให้บุคคลหรือยานพาหนะที่จะผ่านเข้าออกต้องผ่านเฉพาะตามทางเข้าออกที่กำหนดไว้ เพื่อสะดวกในการควบคุมและตรวจสอบ

ซึ่งการระวังป้องกันทางวัตถุประกอบด้วย 2 ส่วนที่สำคัญ ได้แก่

2.1) เครื่องกีดขวาง (Barrier) เครื่องกีดขวางโดย ทั่วไปแบ่งเป็น 2 ชนิด คือ 1) เครื่องกีดขวางตามธรรมชาติ เช่น ทะเล แม่น้ำ ลำคลอง หน้าผา ฯลฯ ที่ได้ดัดแปลงให้เป็นประโยชน์ในการกั้น 2) เครื่องกีดขวางที่ประดิษฐ์ขึ้น เช่น รั้วทึบ รั้วโปร่ง เครื่องกั้นถนน ลวดหีบเพลง กำแพง ลูกกรง เหล็ก ฯลฯ

2.2) การให้แสงสว่าง (Protective lighting) การให้มีแสงสว่างก็เพื่อจะให้มองเห็นบริเวณรั้วและเขตหวงห้ามต่างๆ โดยชัดเจนในเวลามืด จะได้มองเห็นผู้ที่บุกรุกเข้ามาในสถานที่ การให้แสงสว่างมี 2 วิธี คือ 1) การใช้แสงส่องโดยตรง คือ การพุ่งแสงสว่างส่องไปยังจุดใดจุดหนึ่งที่ต้องการ เช่น ที่ตัวอาคาร รั้ว หรือประตู เป็นต้น 2) การใช้แสงส่องกระจายรอบตัว ทำให้มีความสว่างทั่วบริเวณดวงไฟควรอยู่ในระดับสูงพอที่จะช่วยให้

มองเห็นเครื่องกีดขวางต่างๆ ได้ชัด ในกรณีที่รั้วเป็นแบบทึบก็ต้องให้มี แสงสว่างส่องให้เห็นได้ทั้งสองด้าน และต้องให้รัศมีแสงสว่างของดวงหนึ่งๆ ทับเลยเข้าไปในรัศมีของดวงข้างเคียงเพื่อมิให้พื้นที่อับแสงระหว่างรัศมีดวงไฟ (เว็บไซต์กรมพินิจและคุ้มครองเด็กและเยาวชน, 2551)

3) ต้องมีระบบสัญญาณแจ้งเหตุและการสื่อสาร (Alarm & Communication) ซึ่งประกอบด้วย 2 ส่วนที่สำคัญ ได้แก่ ระบบสัญญาณแจ้งเหตุ (Protective alarm) คือ เครื่องมือทางเทคนิคสำหรับตรวจและแจ้งให้ทราบ เมื่อมีการเข้าใกล้หรือล่วงล้ำเข้ามาในพื้นที่ที่มีการรักษาความปลอดภัยที่กำหนดไว้ ระบบสัญญาณแจ้งเหตุนี้อาจเป็นเครื่องมือทางอิเล็กทรอนิกส์ทางไฟฟ้าหรือทางเครื่องกล ที่จะทำให้เกิดสัญญาณเมื่อมีผู้บุกรุก โดยใช้ติดกับประตู หน้าต่าง ตู้เก็บเอกสาร ห้องนิรภัย กำแพง รั้ว พื้นที่ และระบบการสื่อสาร (Communication) เป็นระบบที่ช่วยในการติดต่อ ควบคุม สั่งการ หรือรายงาน ระหว่างเจ้าหน้ารักษาความปลอดภัยกับผู้บังคับบัญชา หรือหน่วยงานที่รับผิดชอบดูแล เช่น ระบบโทรศัพท์ที่ใช้โทรออกได้ทั้งภายในและภายนอก และระบบวิทยุ รวมถึงการสื่อสารประเภทอื่นๆ เช่น ไฟฉาย นกหวีด หรือการใช้เสียงคนก็ได้ แต่ต้องมีการตกลงกันล่วงหน้า

4) ต้องมีระบบควบคุมบุคคลและยานพาหนะ (Personal & Vehicle control) ซึ่งถือเป็นงานหลักของการรักษาความปลอดภัยที่เกี่ยวข้องกับสถานที่ โดยเริ่มจากการพิสูจน์ทราบว่าบุคคลใดมีสิทธิหรือได้รับอนุญาตให้ผ่านเข้าออกในพื้นที่ที่มีการรักษาความปลอดภัยหรือไม่ ซึ่งสามารถแสดงได้โดยบัตรผ่าน (Pass) หรือ ป้ายแสดงตน (Badge) เพื่อเป็นหลักฐานต่อเจ้าหน้าที่รักษาความปลอดภัยขณะที่ผ่านจุดตรวจ

5) ต้องมีระบบเจ้าหน้าที่รักษาความปลอดภัย (Guard force system) คือ เจ้าหน้าที่ผู้มีหน้าที่รับผิดชอบในการรักษาความปลอดภัย ประกอบด้วยเจ้าหน้าที่เวรรักษาความปลอดภัยประจำวัน ยามรักษาการณ์และเจ้าหน้าที่อื่น เจ้าหน้าที่รักษาความปลอดภัยสถานที่จัดขึ้นด้วยความมุ่งหมายเพื่อให้การรักษาความปลอดภัยเกี่ยวกับสถานที่มีประสิทธิภาพยิ่งขึ้น เพราะไม่ว่าจะมีเครื่องกีดขวางชนิดใดหากไม่มีการเฝ้ารักษาแล้ว ก็อาจมีการเล็ดลอดเข้าไปได้ ซึ่งปัจจัยที่นำมาพิจารณากำหนดความต้องการเจ้าหน้าที่รักษาความปลอดภัย ได้แก่ ขนาดที่ตั้ง ผังบริเวณ หรือจุดอ่อนของอาคารสถานที่และจำนวนช่องทางเข้าออก ลักษณะของงานหรือสถานที่ว่ามีความเสี่ยงมากน้อยแค่ไหน จำนวนของบุคคลที่เข้ามาใช้บริการหรือทำงานในสถานที่นั้น จำนวนเขตหวงห้ามและจำนวนยานพาหนะที่ผ่านไปมา และมาตรการต่างๆ ที่ใช้ประกอบการปฏิบัติของเจ้าหน้าที่รักษาความปลอดภัย เช่น ระบบที่ช่วยในการรักษาความปลอดภัยต่างๆ เป็นต้น

6) ต้องมีระบบป้องกัน ระงับอัคคีภัย และหนีไฟ (fire protection, firefighting, & fire escape) หมายถึง การจัดเตรียมเครื่องมืออุปกรณ์ในการดับเพลิง เจ้าหน้าที่ที่รับผิดชอบที่ได้รับการฝึกอบรม ที่สามารถรับมือกับสถานการณ์ได้อย่างทันท่วงที

2.3 ระเบียบสำนักนายกรัฐมนตรีว่าด้วยการรักษาความปลอดภัยแห่งชาติ พ.ศ. 2552

การรักษาความปลอดภัยแห่งชาติ หมายความถึง มาตรการและการดำเนินการที่กำหนดขึ้น เพื่อพิทักษ์รักษาและคุ้มครองป้องกันสิ่งที่เป็นความลับของทางราชการ ตลอดจนหน่วยงานของรัฐ เจ้าหน้าที่ของรัฐ และทรัพย์สินมีค่าของแผ่นดิน ให้พ้นจากการรั่วไหลการจารกรรม การก่อวินาศกรรมการบ่อนทำลาย การก่อการร้าย การกระทำที่เป็นภัยต่อความมั่นคงและผลประโยชน์แห่งรัฐ และการกระทำอื่นใดที่เป็นการเปิดเผยสิ่งที่เป็นความลับของทางราชการ (ระเบียบสำนักนายกรัฐมนตรีว่าด้วยการรักษาความปลอดภัยแห่งชาติ พ.ศ. 2552)

โดยการรักษาความปลอดภัยนั้นมีความมุ่งหมายเพื่อกำหนดหลักการขั้นมูลฐาน และมาตรการในการรักษาความปลอดภัยให้แก่ทางราชการ โดยให้ถือปฏิบัติตามความเหมาะสม และเป็นหลักประกันในด้านการรักษาความปลอดภัย พิทักษ์รักษาและป้องกันสิ่งที่เป็นความลับของทางราชการมิให้รั่วไหลหรือรู้ไปถึง หรือตกไปอยู่กับบุคคลผู้ไม่มีอำนาจหน้าที่ที่จะต้องทราบ การป้องกันการจารกรรม ทั้งจากบุคคลภายในและภายนอกวงราชการ พิทักษ์รักษาและป้องกันการก่อวินาศกรรมแก่บุคคล สิ่งของ อุปกรณ์ อาคาร สถานที่ ฯลฯ และป้องกันการบ่อนทำลายอันจะเป็นผลกระทบกระเทือนต่อความสามัคคี หรือความมั่นคงแห่งชาติ

2.3.1 ประเภทและความรับผิดชอบเกี่ยวกับการรักษาความปลอดภัย

การรักษาความปลอดภัยตามระเบียบนี้แบ่งออกเป็น ประเภท คือ

1. การรักษาความปลอดภัยเกี่ยวกับบุคคล
2. มาตรฐานการรักษาความปลอดภัยเกี่ยวกับข้อมูลข่าวสารลับ
3. มาตรฐานการรักษาความปลอดภัยเกี่ยวกับข้อมูลข่าวสารลับทางระบบอิเล็กทรอนิกส์
4. การรักษาความปลอดภัยเกี่ยวกับสถานที่
5. มาตรฐานการรักษาความปลอดภัยในการประชุมลับ
6. มาตรฐานการปฏิบัติเมื่อเกิดการละเมิดการรักษาความปลอดภัย

1. การรักษาความปลอดภัยเกี่ยวกับบุคคล

การรักษาความปลอดภัยเกี่ยวกับบุคคล เป็นมาตรการที่กำหนดขึ้นสำหรับใช้ปฏิบัติต่อผู้ที่อยู่ระหว่างรอบรรจุ หรือแต่งตั้งเป็นเจ้าหน้าที่ของรัฐ หรือผู้ที่จะได้รับความไว้วางใจให้เข้าถึงสิ่งที่เป็นความลับของทาง

ราชการ หรือให้ปฏิบัติหน้าที่ราชการที่สำคัญ เพื่อเลือกเฟ้น และตรวจสอบ ให้ได้ผู้ที่มีคุณสมบัติเหมาะสมให้เป็นที่เชื่อแน่ว่าต้องเป็นผู้ที่ไม่เป็นภัยต่อความมั่นคงและผลประโยชน์แห่งรัฐ

หัวหน้าหน่วยงานของรัฐต้องจัดให้มีการปฏิบัติ หรือมอบหมายให้มีการปฏิบัติตามมาตรฐานการรักษาความปลอดภัยเกี่ยวกับบุคคล ดังนี้

1. ดำเนินการตรวจสอบประวัติและพฤติการณ์บุคคล ดังนี้

1.1 ผู้ที่อยู่ระหว่างรอบรรจุหรือแต่งตั้งเป็นเจ้าหน้าที่ของรัฐ

1.2 ผู้ที่เป็นลูกจ้างทดลองปฏิบัติงาน หรือฝึกงานก่อนบรรจุเข้าปฏิบัติงาน

1.3 เจ้าหน้าที่ของรัฐที่ยังไม่เคยผ่านการตรวจสอบประวัติและพฤติการณ์ และผู้ที่ขอกลับเข้ารับราชการใหม่

1.4 เจ้าหน้าที่ของรัฐหรือบุคคลที่ได้รับมอบหมายให้ปฏิบัติงานในหน้าที่ หรือตำแหน่งสำคัญของหน่วยงาน หรือเกี่ยวข้องกับสิ่งที่เป็นความลับของทางราชการหรือทรัพย์สิน มีค่าของแผ่นดิน

1.5 ผู้ได้รับทุนการศึกษาทั้งในประเทศหรือต่างประเทศแล้วมีข้อผูกพันให้เข้าปฏิบัติงานให้แก่หน่วยงานของรัฐเมื่อสำเร็จการศึกษา

1.6 บุคคลภายนอกที่เข้ามาปฏิบัติงานให้หน่วยงานของรัฐ

1.7 กรณีตรวจพบบุคคลมีประวัติและพฤติการณ์ต้องสงสัย หรือบุคคลที่เกี่ยวข้องกับชั้นความลับของทางราชการ หัวหน้าหน่วยงานของรัฐอาจขอให้องค์การรักษาความปลอดภัยตรวจสอบเพิ่มเติมได้

2. หน่วยงานของรัฐต้องจัดให้มีการรับรองความไว้วางใจบุคคลที่จะเข้าถึง สิ่งที่เป็นความลับของทางราชการ โดยมีคำสั่งแต่งตั้งเป็นลายลักษณ์อักษร และต้องผ่านการตรวจสอบประวัติและพฤติการณ์

3. เจ้าหน้าที่ควบคุมการรักษาความปลอดภัยหน่วยงานของรัฐ ต้องบันทึกชื่อบุคคลที่ได้รับการรับรองความไว้วางใจไว้ในทะเบียนความไว้วางใจของหน่วยงาน

4. หัวหน้าหน่วยงานของรัฐต้องจัดให้มีการอบรมชี้แจงเกี่ยวกับระเบียบการรักษาความปลอดภัยแก่บุคคลที่ได้รับการบรรจุใหม่ ผู้ที่ไม่เคยได้รับการอบรม หรือผู้ที่จะได้รับมอบหมายให้ปฏิบัติหน้าที่เกี่ยวกับความลับของทางราชการ รวมถึงการให้ความรู้ในวิทยาการด้านต่าง ๆ และต้องอบรมทบทวนตามระยะเวลาที่เหมาะสม เพื่อกระตุ้นจิตสำนึกและวินัยในด้านการรักษาความปลอดภัย

2.3.2 การปฏิบัติตามมาตรฐานการรักษาความปลอดภัยเกี่ยวกับบุคคล

บุคคลเป็นปัจจัยสำคัญที่สุดในการปฏิบัติตามมาตรการรักษาความปลอดภัยทุกด้านให้สำเร็จและมีประสิทธิภาพ อย่างไรก็ดี บุคคลอาจเป็นต้นเหตุที่ก่อให้เกิดความเสียหายต่อระบบการรักษาความปลอดภัยได้เช่นกัน ฉะนั้น การรักษาความปลอดภัยเกี่ยวกับบุคคลจึงกำหนดขึ้น เพื่อคัดกรอง ตรวจสอบบุคคลที่จะเข้าปฏิบัติงานให้กับหน่วยงานของรัฐ เพื่อให้ ได้ผู้ที่มีคุณสมบัติเหมาะสม และมีความประพฤติที่ไม่เสียหาย หรือเป็นภัยต่อความมั่นคงและผลประโยชน์แห่งรัฐ

1. การตรวจสอบประวัติและพฤติการณ์บุคคล

บุคคลที่ต้องได้รับการตรวจสอบประวัติและพฤติการณ์ คือ ผู้ได้รับการบรรจุเป็นเจ้าหน้าที่ใหม่ของรัฐ เจ้าหน้าที่ของรัฐที่ยังไม่เคยผ่านการตรวจสอบประวัติและพฤติการณ์ ผู้ที่ขอกลับเข้ารับราชการ นักเรียน นักศึกษา นิสิตของหน่วยงานของรัฐ ที่มีข้อผูกพันว่าจะได้รับการบรรจุเข้าทำงานในหน่วยงานของรัฐนั้น ๆ บุคคลที่ได้รับมอบหมายให้ปฏิบัติงานในหน่วยงานของรัฐ เช่น พนักงานที่จัดจ้างจากบริษัทภายนอก บุคคลที่ได้รับการแต่งตั้งให้ดำรงตำแหน่งสำคัญ ตามความเหมาะสมของภารกิจในหน่วยงานของรัฐ บุคคลที่มีพฤติการณ์หรือปรากฏข่าวสาร หรือติดต่อกับบุคคล หรือองค์กรที่อาจเป็นภัยต่อความมั่นคงของประเทศ เจ้าหน้าที่ของรัฐที่เข้าถึงเรื่องลับที่สุด ลับมาก ลับ หรือการรหัส

การตรวจสอบประวัติและพฤติการณ์บุคคล หน่วยงานของรัฐนั้น ๆ ดำเนินการตรวจสอบเองได้ โดยขอคำแนะนำจากองค์การรักษาความปลอดภัย เพื่อให้ได้บุคคล ที่มีคุณสมบัติครบถ้วนตรงตามวัตถุประสงค์ของหน่วยงานและตามกฎหมายหรือระเบียบข้อบังคับ

2.3.3 แนวทางการตรวจสอบประวัติและพฤติการณ์บุคคล

1. การตรวจสอบเบื้องต้น

1.1 ตรวจสอบบุคคลที่อยู่ระหว่างรอบรรจุหรือแต่งตั้งเป็นเจ้าหน้าที่ของรัฐ ผู้ที่เป็นลูกจ้างทดลองปฏิบัติงาน หรือฝึกงานก่อนบรรจุเข้าปฏิบัติงาน เจ้าหน้าที่ของรัฐที่ยังไม่เคยผ่านการตรวจสอบประวัติและพฤติการณ์ ผู้ที่พ้นจากภารกิจ หรือตำแหน่งหน้าที่แล้ว แต่ต้องกลับเข้าทำงานที่เกี่ยวข้องกับชั้นความลับของทางราชการ ผู้ที่ขอกลับเข้ารับราชการใหม่เจ้าหน้าที่ของรัฐหรือบุคคลที่ได้รับมอบหมายให้ปฏิบัติงานในหน้าที่ หรือตำแหน่งสำคัญของหน่วยงาน หรือเกี่ยวข้องกับสิ่งที่เป็นความลับของทางราชการหรือทรัพย์สิน มีค่าของแผ่นดิน ผู้ได้รับทุนการศึกษาทั้งในประเทศหรือต่างประเทศแล้วมีข้อผูกพันให้เข้าปฏิบัติงานให้แก่หน่วยงานของรัฐเมื่อสำเร็จการศึกษา และบุคคลภายนอกที่เข้ามาปฏิบัติงานให้หน่วยงานของรัฐ

1.2 วิธีการตรวจสอบเบื้องต้น ให้มีการปฏิบัติดังนี้

1.2.1 จัดพิมพ์รายชื่อบุคคลที่จะต้องตรวจสอบ หมายเลขบัตร ประจำตัวประชาชน วัน เดือน ปีเกิด ที่อยู่ ชื่อ-สกุลของบิดา/มารดา ส่งกองทะเบียนประวัติอาชญากร สำนักงานตำรวจแห่งชาติ เพื่อตรวจสอบข้อมูลด้านอาชญากรรม

1.2.2 ให้บุคคลที่จะต้องตรวจสอบไปพิมพ์ลายนิ้วมือที่สถานีตำรวจท้องที่ที่บุคคลผู้นั้นมีภูมิลำเนาอยู่ การจัดพิมพ์ลายนิ้วมือนั้นเพื่อส่งให้สำนักงานตำรวจแห่งชาติดำเนินการตรวจสอบประวัติอาชญากรรม และพฤติการณ์อื่นที่สถานีตำรวจท้องที่นั้น ๆ บันทึกเก็บไว้

1.2.3 หน่วยงานของรัฐให้ผู้ถูกตรวจสอบกรอกแบบประวัติบุคคล ให้ครบถ้วน และอยู่ภายใต้การดูแลของเจ้าหน้าที่ควบคุมการรักษาความปลอดภัยประจำหน่วยงานของรัฐหรือเจ้าหน้าที่ผู้รับผิดชอบจัดส่งให้องค์การรักษาความปลอดภัยเพื่อตรวจสอบข้อมูลด้านความมั่นคง

2. การตรวจสอบโดยละเอียด

2.1 การตรวจสอบบุคคลที่จะเข้าถึงสิ่งที่เป็นความลับของทางราชการชั้นลับที่สุด ลับมาก ลับ หรือการรหัส บุคคลที่มีพฤติการณ์ หรือปรากฏข่าวสาร หรือติดต่อกับบุคคล หรือองค์การทั้งภายในและภายนอกประเทศ ที่จะเป็นภัย หรือเสี่ยงต่อความมั่นคงและผลประโยชน์แห่งรัฐ บุคคลที่จะได้รับมอบหมายให้ทำหน้าที่หรือแต่งตั้งให้ดำรงตำแหน่งสำคัญในหน่วยงานของรัฐ ต้องได้รับการตรวจสอบโดยละเอียด

2.2 วิธีการตรวจสอบโดยละเอียด

2.2.1 ให้เป็นไปตามหลักเกณฑ์และวิธีการที่กำหนดในประกาศสำนัก นายกรัฐมนตรี

2.2.2 การตรวจสอบโดยละเอียดอาจขอให้องค์การรักษาความปลอดภัยดำเนินการให้ โดยปฏิบัติตามหลักเกณฑ์ที่องค์การรักษาความปลอดภัยกำหนด

2.2.3 กรณีขอให้องค์การรักษาความปลอดภัยตรวจสอบประวัติและ พฤติการณ์บุคคล ให้หน่วยงานของรัฐส่งหนังสือนำพร้อมแบบประวัติบุคคลของบุคคลที่จะต้องตรวจสอบโดยระบุวัตถุประสงค์ในการตรวจสอบ ในกรณีที่เคยผ่านการตรวจสอบประวัติและพฤติการณ์มาแล้ว ให้ระบุชื่อหน่วยงานที่เคยดำเนินการตรวจสอบประวัติและพฤติการณ์ด้วย

3. ในระหว่างที่รอฟังผลการตรวจสอบประวัติและพฤติการณ์บุคคล ถ้าจำเป็นต้องรีบบรรจุหรือจ้างบุคคลเข้าปฏิบัติงาน ก็ให้บรรจุหรือจ้างก่อนได้ โดยมีเงื่อนไขว่า ถ้าผลการตรวจสอบปรากฏว่าผู้นั้นมีความประพฤติหรือมีประวัติและพฤติการณ์ไม่เหมาะสมให้หน่วยงานของรัฐสั่งเลิกบรรจุหรือเลิกจ้างได้

4. ถึงแม้ว่าหัวหน้าหน่วยงานของรัฐจัดให้มีการตรวจสอบประวัติและพฤติการณ์ของผู้ใต้บังคับบัญชาแล้วนั้น เพื่อให้การรักษาความปลอดภัยมีประสิทธิภาพอยู่เสมอ หากพบว่า เจ้าหน้าที่ของรัฐผู้ใดมีพฤติการณ์ที่น่าสงสัยหรือมีการกระทำอันก่อให้เกิดความไม่น่าไว้วางใจซึ่งอาจเป็นภัยต่อความมั่นคงและผลประโยชน์แห่งรัฐ ให้ย้ายผู้นั้นออกจากตำแหน่งหน้าที่นั้นโดยเร็วและพิจารณาดำเนินการต่อไป โดยให้รายงานองค์การรักษาความปลอดภัยทราบ หรือขอให้ตรวจสอบประวัติพฤติการณ์ใหม่

2. การรับรองความไว้วางใจบุคคลเพื่อให้เข้าถึงสิ่งที่เป็นความลับของทางราชการ

หัวหน้าหน่วยงานของรัฐเป็นผู้พิจารณารับรองความไว้วางใจให้เจ้าหน้าที่ของรัฐหรือบุคคลที่จะเข้าถึงสิ่งที่เป็นความลับของทางราชการ หรือปฏิบัติหน้าที่สำคัญ โดยให้ปฏิบัติดังนี้

2.1 บุคคลที่ได้รับการรับรองความไว้วางใจ ต้องผ่านการตรวจสอบประวัติและพฤติการณ์ โดยได้รับการอนุมัติจากหัวหน้าหน่วยงานของรัฐและให้เจ้าหน้าที่ควบคุมการรักษาความปลอดภัยบันทึกในแบบการรับรองความไว้วางใจ

2.2 บุคคลใดที่ได้รับการรับรองความไว้วางใจ ต้องผ่านการอบรม หรือชี้แจงในเรื่องการรักษาความปลอดภัย เพื่อให้สามารถปฏิบัติหน้าที่ที่ได้รับมอบหมายให้ถูกต้อง และมีจิตสำนึกในการรักษาความปลอดภัย

2.3 บุคคลที่ได้รับความไว้วางใจ จะต้องลงนามในบันทึกรับรองการรักษาความลับ เมื่อเข้ารับตำแหน่งหน้าที่ และเมื่อพ้นตำแหน่งหน้าที่ให้ลงนามในบันทึกรับรองการรักษาความลับ เพื่อสัญญาว่าจะรักษาความลับของทางราชการ และไม่นำไปเปิดเผยให้ผู้ไม่มีอำนาจหน้าที่เกี่ยวข้องได้รับทราบการรับรองความไว้วางใจบุคคลให้เข้าถึงความลับชั้นต่าง ๆ หรือหน้าที่สำคัญไม่มีข้อจำกัดในเรื่องตำแหน่ง ระดับ ยศ แต่อย่างใด กรณีเกิดความจำเป็นหัวหน้าหน่วยงานของรัฐพิจารณาเห็นว่าบุคคลผู้นั้นมีความเหมาะสม โดยดำเนินกรรมวิธีการรับรองความไว้วางใจตามที่ระเบียบกำหนดไว้

2.4 เมื่อมีความจำเป็นเร่งด่วน หัวหน้าหน่วยงานของรัฐอาจรับรองความไว้วางใจบุคคล ก่อนทราบผลการตรวจสอบประวัติและพฤติการณ์ ในกรณีดังนี้

2.4.1 บุคคลที่มีความจำเป็นต้องรีบบรรจุหรือว่าจ้าง

2.4.2 บุคคลปฏิบัติหน้าที่เฉพาะภารกิจเป็นการชั่วคราวที่เกี่ยวกับความลับของทางราชการ

3. การทะเบียนความไว้วางใจ

เจ้าหน้าที่ควบคุมการรักษาความปลอดภัยหน่วยงานของรัฐ จะต้องลงทะเบียนความไว้วางใจของเจ้าหน้าที่ในหน่วยงานของตนที่ได้รับความไว้วางใจ โดยยึดถือใบรับรองความไว้วางใจ เป็นหลักฐาน และมีการตรวจสอบข้อมูลให้ถูกต้องตามความเป็นจริงอยู่เสมอ เมื่อพบบุคคลใดมีพฤติการณ์ที่น่าสงสัย ต้องตรวจสอบประวัติและพฤติการณ์ เพิ่มเติม หากปรากฏพฤติการณ์เป็นที่ไม่น่าไว้วางใจ ให้ยกเลิกหรือลดระดับความไว้วางใจ พร้อมบันทึกการเปลี่ยนแปลงในทะเบียนความไว้วางใจทุกครั้ง

กรณีที่พ้นจากตำแหน่งหรือหน้าที่ที่เกี่ยวข้องกับสิ่งที่เป็นความลับของทางราชการในชั้นลับที่สุดลับมาก และลับ ต้องคัดชื่อบุคคลนั้นออกจากทะเบียนความไว้วางใจด้วย และให้บุคคลนั้นส่งคืนข้อมูลข่าวสารและหลักฐานต่างๆ ในความรับผิดชอบทั้งหมด และเจ้าหน้าที่ควบคุมการรักษาความปลอดภัยประจำหน่วยงานของรัฐต้องชี้แจงให้ทราบถึงความรับผิดชอบในการรักษาความลับของทางราชการ พร้อมกับให้บุคคลนั้นลงลายมือชื่อในบันทึกรับรองการรักษาความลับ เมื่อพ้นตำแหน่งหรือหน้าที่ไว้เป็นหลักฐาน

4. การอบรมเรื่องการรักษาความปลอดภัย

การมีจิตสำนึกและวินัยในการรักษาความปลอดภัย มีความสำคัญอย่างยิ่งต่อการรักษาความปลอดภัยในหน่วยงานของรัฐ ดังนั้นหน่วยงานของรัฐ จึงควรจัดให้มีการปฏิบัติดังนี้

4.1 หัวหน้าหน่วยงานของรัฐต้องจัดให้มีการอบรมชี้แจงระเบียบเกี่ยวกับการรักษาความปลอดภัยแก่เจ้าหน้าที่ของรัฐ บุคคลที่จะปฏิบัติหน้าที่เกี่ยวข้องกับความลับของทางราชการ และบุคคลที่ต้องเข้ามาปฏิบัติงานในพื้นที่ควบคุม ให้มีความรู้ความเข้าใจเกี่ยวกับเรื่องการรักษาความปลอดภัย

4.2 ต้องมีการอบรม ทบทวนเกี่ยวกับการรักษาความปลอดภัย และเพิ่มเติมวิทยาการใหม่ตามห้วงเวลาที่เหมาะสม เพื่อกระตุ้นจิตสำนึกและวินัยในการรักษาความปลอดภัย

4.3 หน่วยงานของรัฐอาจประสานขอความร่วมมือ และคำแนะนำในการจัดอบรมให้ความรู้จากองค์การรักษาความปลอดภัยได้

2. มาตรฐานการรักษาความปลอดภัยเกี่ยวกับข้อมูลข่าวสารลับ

เป็นการคุ้มครองข้อมูลข่าวสารลับไม่ให้สูญหาย ถูกทำลาย เปลี่ยนแปลง หรือ รั่วไหล การเปิดเผยข้อมูลข่าวสารลับต่อบุคคลผู้ไม่มีอำนาจหน้าที่ต้องอยู่ภายใต้เงื่อนไข โดยมีข้อยกเว้นที่ชัดเจนสอดคล้องกับพระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ.2540 และระเบียบว่าด้วยการรักษาความลับของทางราชการ พ.ศ.2544

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

มาตรฐานการรักษาความปลอดภัยเกี่ยวกับข้อมูลข่าวสารลับ หัวหน้าหน่วยงานของรัฐต้องจัดให้มีการปฏิบัติดังนี้

1. หัวหน้าหน่วยงานของรัฐต้องมีคำสั่งแต่งตั้งเป็นลายลักษณ์อักษร และให้การรับรองความไว้วางใจแก่บุคคลที่เกี่ยวข้องกับการดำเนินการต่อข้อมูลข่าวสารลับ ดังนี้

1.1 นายทะเบียนข้อมูลข่าวสารลับและผู้ช่วยนายทะเบียนข้อมูลข่าวสารลับ ทำหน้าที่ดำเนินการเกี่ยวกับข้อมูลข่าวสารลับ

1.2 ผู้มีอำนาจในการกำหนดชั้นความลับ

1.3 คณะกรรมการดำเนินการเกี่ยวกับข้อมูลข่าวสารลับ ประกอบด้วย คณะกรรมการ ตรวจสอบข้อมูลข่าวสารลับ คณะกรรมการทำลายข้อมูลข่าวสารลับ

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

2.1 การกำหนดชั้นความลับและแสดงเหตุผล หน่วยงานของรัฐที่มีข้อมูลข่าวสารลับ ต้องมีการกำหนดชั้นความลับให้ข้อมูลข่าวสารนั้น โดยต้องระบุเหตุผลย่อ (ให้สอดคล้องกับข้อมูลข่าวสารที่ไม่ต้องเปิดเผยตามมาตรา 14 และ15 ตามพระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ.2540) ของการกำหนดชั้นความลับนั้นไว้ในทะเบียนควบคุมข้อมูลข่าวสารลับ ต้องแสดงชั้นความลับให้เห็นชัดเจน ข้อมูลข่าวสารลับสามารถ ปรับลด เพิ่ม ยกเลิก ชั้นความลับได้ โดยหน่วยงานเจ้าของเรื่อง เดิม ผู้มีอำนาจกำหนดชั้นความลับของข้อมูลข่าวสารลับนั้น

2.2 การจัดทำข้อมูลข่าวสารลับ

2.2.1 กำหนดจำนวนเจ้าหน้าที่ที่เกี่ยวข้องและจำกัดให้ทราบเท่าที่จำเป็น

2.2.2 มีการคุมชุดข้อมูลข่าวสารลับ

2.3 หน่วยงานของรัฐที่ครอบครองข้อมูลข่าวสารลับ สามารถ สำเนา แปล เข้ารหัส หรือถอดรหัสข้อมูลข่าวสารลับเองได้ โดยต้องบันทึกรายละเอียดไว้ที่ต้นฉบับ และฉบับที่ดำเนินการสำเนา แปล เข้าหรือถอดรหัสด้วย การส่ง การรับ ข้อมูลข่าวสารลับ

2.4 การโอนข้อมูลข่าวสารลับภายในหน่วยงาน หรือ ระหว่างหน่วยงานต้องได้รับการอนุมัติจากหัวหน้าหน่วยงานของรัฐ และบันทึกการโอนไว้ในทะเบียนควบคุมข้อมูลข่าวสารลับ

2.5 การส่ง การรับ ข้อมูลข่าวสารลับ

2.5.1 การส่งข้อมูลข่าวสารลับภายในหน่วยงาน ต้องใช้ใบปกข้อมูลข่าวสารลับปิดทับข้อมูลข่าวสารลับ และการส่งออกนอกหน่วยงานต้องบรรจุซอง หรือภาชนะทึบแสงสองชั้นอย่างมั่นคง และแยกทะเบียนข้อมูลข่าวสารลับ ออกจากทะเบียน รับ- ส่ง ข้อมูลข่าวสารที่ไม่มีชั้นความลับ

2.5.2 การรับข้อมูลข่าวสารลับ ต้องให้นายทะเบียนข้อมูลข่าวสารลับ หรือผู้ช่วยนายทะเบียนข้อมูลข่าวสารลับ ลงชื่อในใบตอบรับแล้วส่งคืนใบตอบรับนั้นแก่ผู้นำส่ง หรือจัดส่งคืนภายหลัง และลงทะเบียนข้อมูลข่าวสารลับก่อนที่จะดำเนินการต่อไป

2.6 การเก็บรักษาข้อมูลข่าวสารลับ หน่วยงานของรัฐต้องเก็บรักษาไว้ในที่ปลอดภัย และควรกำหนดระเบียบการเก็บรักษาข้อมูลข่าวสารลับของหน่วยงานตนเองเพิ่มเติม

2.7 การยืมข้อมูลข่าวสารลับของหน่วยงานอื่น ต้องได้รับอนุญาตจากหน่วยงานเจ้าของเรื่อง ยกเว้นเป็นการขอยืมภายในหน่วยงานเจ้าของเรื่อง และต้องบันทึกการยืมไว้ในทะเบียนควบคุมข้อมูลข่าวสารลับ

2.8 การทำลายข้อมูลข่าวสารลับทุกชั้นความลับ ต้องส่งให้หอจดหมายเหตุแห่งชาติพิจารณาก่อนทำลาย ยกเว้นข้อมูลข่าวสารลับ ชั้นลับที่สุด ที่เสี่ยงต่อการรั่วไหล อันก่อให้เกิดอันตรายแก่ประโยชน์แห่งรัฐ หัวหน้าหน่วยงานของรัฐอาจพิจารณาทำลายเองได้

2.9 หากข้อมูลข่าวสารลับสูญหาย ต้องรายงานให้หัวหน้าหน่วยงานของรัฐที่ตนสังกัดและหน่วยงานเจ้าของเรื่องเดิมทราบ เพื่อดำเนินการตรวจสอบและสอบสวนข้อเท็จจริง และจดแจ้งการสูญหายไว้ในทะเบียนควบคุมข้อมูลข่าวสารลับ

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

2.10.1 การเปิดเผยข้อมูลข่าวสารลับโดยหัวหน้าหน่วยงานของรัฐ หรือเจ้าหน้าที่ของรัฐตาม ม.20 (1) แห่งพระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ.2540 2.10.2 การเปิดเผยข้อมูลข่าวสารลับกรณีคำวินิจฉัยของคณะกรรมการวินิจฉัยการเปิดเผยข้อมูลข่าวสารลับ

3. หน่วยงานของรัฐต้องจัดให้มีแผนการปฏิบัติต่อข้อมูลข่าวสารลับในเวลาปกติและเวลาฉุกเฉิน เพื่อป้องกันการเข้าถึงของบุคคลที่ไม่มีอำนาจหน้าที่ โดยจัดทำแผนดังนี้

3.1 แผนเคลื่อนย้ายข้อมูลข่าวสารลับ

3.2 แผนการพิทักษ์รักษา

3.3 แผนการทำลาย

2.3.3 การปฏิบัติตามมาตรฐานการรักษาความปลอดภัยเกี่ยวกับข้อมูลข่าวสารลับ

เพื่อเป็นการป้องกันข้อมูลข่าวสารลับหน่วยงานของรัฐไม่ให้สูญหาย ถูกทำลายเปลี่ยนแปลง หรือรั่วไหล และป้องกันการเข้าถึงของผู้ที่ไม่มีอำนาจหน้าที่ หน่วยงานของรัฐควรปฏิบัติดังนี้

1. หัวหน้าหน่วยงานของรัฐต้องมีคำสั่งแต่งตั้งเป็นลายลักษณ์อักษรให้บุคคลปฏิบัติหน้าที่ต่าง ๆ เป็น ลายลักษณ์อักษร ดังนี้

1.1 นายทะเบียนข้อมูลข่าวสารลับ และผู้ช่วยนายทะเบียนข้อมูลข่าวสารลับ มีหน้าที่ดังนี้

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

1.1.2 จัดเก็บแบบทะเบียนต่าง ๆ และข้อมูลข่าวสารลับที่อยู่ในความควบคุมดูแลให้ปลอดภัย

1.1.3 เก็บรักษาบัญชีรายมือชื่อนายทะเบียนข้อมูลข่าวสารลับ และผู้ช่วยนายทะเบียนข้อมูลข่าวสารลับ ของหน่วยงานของรัฐที่ติดต่อเกี่ยวข้องกันเป็นประจำ

1.2 ผู้มีอำนาจในการกำหนดชั้นความลับ

1.3 คณะกรรมการดำเนินการเกี่ยวกับข้อมูลข่าวสารลับ ประกอบด้วยคณะกรรมการตรวจสอบและคณะกรรมการทำลายข้อมูลข่าวสารลับ ซึ่งมีนายทะเบียนข้อมูลข่าวสารลับเป็นประธาน และเจ้าหน้าที่ไม่น้อยกว่า 2 คน เป็นกรรมการ คณะกรรมการทั้งสองชุดดังกล่าวเป็นคนละชุดกันยกเว้นประธานกรรมการ

คณะกรรมการตรวจสอบความถูกต้องในการปฏิบัติตามระเบียบ การมีอยู่ของข้อมูลข่าวสารตามทะเบียนข้อมูลข่าวสาร อย่างน้อยทุก 6 เดือน และข้อมูลข่าวสารลับที่ไม่ประสงค์จะเก็บรักษา และ ข้อมูลข่าวสารลับที่ครบอายุการเก็บรักษาตาม มาตรา 14 และ มาตรา 15 แห่งพระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ.2540

2. การดำเนินการเกี่ยวกับข้อมูลข่าวสารลับ หัวหน้าหน่วยงานของรัฐ อาจมอบหมายการกำหนดชั้นความลับให้ผู้ใต้บังคับบัญชาได้ โดยมีคำสั่งมอบหมายเป็น ลายลักษณ์อักษร

2.1 การกำหนดชั้นความลับและแสดงเหตุผล

2.1.1 การกำหนดชั้นความลับต้องคำนึงถึงข้อมูลข่าวสารที่ไม่ต้องเปิดเผยตามมาตรา 15 แห่ง พ.ร.บ.ข้อมูลข่าวสารของราชการ พ.ศ.2540 และปฏิบัติตามระเบียบว่าด้วยการรักษาความลับของทางราชการ พ.ศ.2544 กำหนดให้พิจารณาถึงองค์ประกอบในการกำหนดชั้นความลับดังต่อไปนี้

1) ความสำคัญของเนื้อหา

2) แหล่งที่มาของข้อมูล

3) วิธีการนำไปใช้ประโยชน์

4) จำนวนบุคคลที่รับทราบ

5) ผลกระทบหากมีการเปิดเผย

6) หน่วยงานของรัฐที่รับผิดชอบในฐานะเจ้าของเรื่องหรืออนุมัติในการกำหนดชั้นความลับของข้อมูลข่าวสาร

2.1.2 การแสดงชั้นความลับต้องให้เห็นเด่นชัด ทั้งข้อมูลข่าวสารที่มีสภาพเป็นกระดาษ เอกสารม้วน หรือพับ จานบันทึก แถบบันทึก หรือข้อมูลข่าวสารลับที่อยู่ในรูปแบบอื่น ๆ

2.1.3 การปรับชั้นความลับ (ปรับลด เพิ่ม หรือยกเลิกชั้นความลับ) ต้องกระทำโดยผู้กำหนดชั้นความลับของหน่วยงานเจ้าของเรื่อง และต้องแจ้งให้หน่วยงานของรัฐอื่นที่ได้รับการแจกจ่ายทราบ เพื่อแก้ไขชั้นความลับด้วยทุกครั้ง

2.2 การจัดทำข้อมูลข่าวสารลับ ควรดำเนินการ ดังนี้

2.2.1 กำหนดจำนวนเจ้าหน้าที่ที่เกี่ยวข้อง และจำกัดให้ทราบเท่าที่จำเป็น ซึ่งบุคคลผู้นั้นต้องได้รับความไว้วางใจไม่ต่ำกว่าชั้นความลับของข้อมูลข่าวสารลับนั้น

2.2.2 การจัดทำต้องทำในสถานที่ที่ปลอดภัย

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

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

2.3 หน่วยงานของรัฐที่ครอบครองข้อมูลข่าวสารลับใดอยู่ หมายรวมถึงฉบับที่ตนเป็นเจ้าของเรื่อง หรือฉบับที่ได้รับการแจกจ่ายมาจากหน่วยงานอื่น ให้รับผิดชอบในการจัดทำสำเนาเพิ่มเติม หรือการแปลเอง โดยให้บันทึกจำนวนที่สำเนาเพิ่ม และทำบัญชีรายการแจกจ่ายไว้ด้วย เพื่อการควบคุมและตรวจสอบกรณีเกิดการละเมิดการรักษาความลับ หรือเมื่อข้อมูลข่าวสารลับรั่วไหล

2.4 การโอนข้อมูลข่าวสารลับจะกระทำได้ต่อเมื่อผู้โอน และผู้รับโอนได้รับอนุมัติจากหัวหน้าหน่วยงานของรัฐ และต้องดำเนินการโดยมีหลักฐานเป็นลายลักษณ์อักษร เมื่อดำเนินการแล้วทั้งผู้โอน และผู้รับโอน ต้องรายงานให้หัวหน้าหน่วยงานของตนทราบ

การโอนข้อมูลข่าวสารลับระหว่างหน่วยงานของรัฐ หรือการโอนข้อมูลข่าวสารลับภายในหน่วยงานเดียวกัน ควรปฏิบัติดังนี้

1. เจ้าหน้าที่ผู้โอน และผู้รับโอนต้องจัดทำบันทึกการโอน และบุคคลดังกล่าวต้องได้รับความไว้วางใจไม่ต่ำกว่าชั้นความลับของข้อมูลข่าวสารลับนั้น

2. นายทะเบียนข้อมูลข่าวสารลับ ต้องจดแจ้งการโอนในทะเบียนควบคุมข้อมูลข่าวสารลับ

2.5 การส่ง การรับ ข้อมูลข่าวสารลับ ดำเนินการดังนี้

การส่งข้อมูลข่าวสารลับ

2.5.1 การส่งข้อมูลข่าวสารลับภายในหน่วยงานให้ใช้ใบปกข้อมูล ข่าวสารลับปิดทับข้อมูลข่าวสารลับ เพื่อให้ผู้ไม่มีหน้าที่เกี่ยวข้องได้เห็นข้อความภายใน และเป็นการเตือนให้รักษาความลับของทาง

ราชการ ผู้ส่งต้องกระทำโดยเจ้าหน้าที่ผู้รับผิดชอบ และได้รับความไว้วางใจไม่ต่ำกว่าชั้นความลับของข้อมูลข่าวสารลับนั้น

2.5.2 การส่งข้อมูลข่าวสารลับออกนอกบริเวณหน่วยงาน หมายความรวมถึงการส่งให้แก่หน่วยงานอื่น และการส่งให้หน่วยงานเดียวกันแต่ไม่ได้อยู่บริเวณเดียวกัน ควรปฏิบัติดังนี้

1) ข้อมูลข่าวสารลับต้องบรรจุซองทึบแสงสองชั้น และให้แนบใบตอบรับไว้ที่หน้าซองชั้นในของข้อมูลข่าวสารลับนั้น

2) บนซองชั้นใน ให้จ่าหน้า

- ระบุเลขที่หนังสือนำส่ง
- ชื่อหรือตำแหน่งผู้รับ
- หน่วยงานผู้ส่ง
- ทำเครื่องหมายแสดงชั้นความลับทั้งด้านหน้าและด้านหลัง
- สำหรับข้อมูลข่าวสารลับ ชั้นลับที่สุด และลับมากที่มีการระบุชื่อผู้รับ ให้บุคคลตามที่ระบุชื่อเป็นผู้เปิดซองนั้น

3) ผู้ปิดผนึกซอง ต้องเป็นผู้มีอำนาจหน้าที่ การปิดผนึก และลงลายมือชื่อของผู้ปิดผนึกไว้บนรอยปิดผนึกของซอง และใช้แถบกาวชนิดใสปิดทับ เพราะแถบกาวใสจะช่วยให้สามารถตรวจสอบร่องรอยการลอบเปิดซอง หรือห่อชั้นในได้ง่าย

4) บนซองชั้นนอก ให้จ่าหน้าเหมือนซองชั้นใน แต่ไม่ต้องแสดงชั้นความลับ

การรับข้อมูลข่าวสารลับ

ใบตอบรับ ที่แนบไว้หน้าซองชั้นใน ไม่ต้องระบุชั้นความลับ และชื่อเรื่อง ระบุเฉพาะเลขที่หนังสือ วัน เดือน ปี จำนวนหน้า และหมายเลขฉบับ ผู้รับจะส่งคืนใบตอบรับตามสายงานของการส่งหนังสือ หากให้เจ้าหน้าที่นำสารถือข้อมูลข่าวสารลับไปเองให้รอรับใบตอบรับคืนด้วย

2.6 การเก็บรักษาข้อมูลข่าวสารลับ

2.6.1 ข้อมูลข่าวสารลับที่มีสภาพเป็นเอกสาร ให้เจ้าหน้าที่ผู้ครอบครอง ควบคุมดูแล เก็บข้อมูลข่าวสารลับเหล่านั้นไว้ในแฟ้มข้อมูลข่าวสารลับ และเก็บแฟ้มข้อมูลข่าวสารลับไว้ในตู้เก็บข้อมูลข่าวสารลับโดยแยกเป็นเฉพาะเรื่อง

2.6.2 ตู้เก็บข้อมูลข่าวสารลับควรเป็นตู้เหล็ก ปิดล็อคด้วยกุญแจที่มั่นคง 2.6.3 ควรลง วัน เดือน ปี เวลา เปิด-ปิด ตู้เก็บรักษาข้อมูลข่าวสารลับและลงลายมือชื่อ ของผู้เปิด-ปิด และเวลาเปิด-ปิดไว้ด้วย

2.6.4 ตู้เก็บข้อมูลข่าวสารลับต้องเก็บไว้ในสถานที่ ซึ่งมีระบบการรักษาความปลอดภัยเกี่ยวกับสถานที่ ที่กำหนดให้เป็น “พื้นที่หวงห้าม”

2.6.5 ควรจัดให้มีตู้เก็บลูกกุญแจรวม เพื่อเป็นที่เก็บลูกกุญแจตู้เก็บข้อมูลข่าวสารลับทุกตู้รวมไว้ที่เดียวกัน ตู้เก็บลูกกุญแจรวม ควรปิดล็อคด้วยกุญแจที่มีความมั่นคงกว่าตู้เก็บข้อมูลข่าวสารลับ และจัดที่เก็บไว้ในที่ที่เหมาะสม

2.6.6 นายทะเบียนข้อมูลข่าวสารลับ ดูแลตู้เก็บลูกกุญแจรวม โดยผู้ที่ รับผิดชอบ ตู้ข้อมูลข่าวสารลับ ควรนำลูกกุญแจตู้ที่ตนรับผิดชอบทั้งหมดมาเก็บไว้ในตู้เก็บกุญแจรวมหลังเสร็จภารกิจประจำวัน

2.6.7 การเก็บข้อมูลข่าวสารลับไว้ในเครื่องคอมพิวเตอร์จะต้องจัดเก็บลงในสื่อบันทึกข้อมูล เช่น แผ่นดิสก์ ซีดีรอม เทปบันทึก หรืออุปกรณ์อื่นที่ใช้จัดเก็บข้อมูลด้วยเครื่องคอมพิวเตอร์ โดยมีระบบรักษาความปลอดภัยในการจัดเก็บ และเรียกใช้ข้อมูลด้วยระบบรหัสผู้ใช้ และรหัสผ่าน

2.7 การยืมข้อมูลข่าวสารลับ ให้หัวหน้าหน่วยงานของรัฐ หรือผู้ได้รับมอบหมายเป็นผู้พิจารณาตรวจสอบคุณสมบัติของผู้ยืมว่า เป็นผู้มีอำนาจหน้าที่เกี่ยวข้อง ได้รับความไว้วางใจให้เข้าถึงชั้นความลับของข้อมูลข่าวสารที่จะยืม และสามารถปฏิบัติตามระเบียบว่าด้วยการรักษาความลับของทางราชการ พ.ศ.2544 ได้ พร้อมทั้งต้องบันทึกหลักฐานการยืมในทะเบียนควบคุมข้อมูลข่าวสารลับ

2.8 ข้อมูลข่าวสารลับของหน่วยงานของรัฐที่ไม่ประสงค์จะเก็บรักษา หรือมีอายุครบกำหนดการเก็บ ต้องส่งให้หอจดหมายเหตุแห่งชาติ กรมศิลปากร พิจารณาคัดเลือกไว้ให้ประชาชนได้ศึกษา ค้นคว้า ตามมาตรา 26 แห่ง พ.ร.บ.ข้อมูลข่าวสารของราชการ พ.ศ.2540 การทำลายให้พิจารณาจาก

2.8.1 ข้อมูลข่าวสารลับที่หอจดหมายเหตุแห่งชาติ พิจารณาแล้วว่าไม่มีคุณค่าในการเก็บรักษา

2.8.2 ข้อมูลข่าวสารลับ ชั้น “ลับที่สุด” ที่หากเก็บรักษาไว้จะเสี่ยงต่อการรั่วไหล อันอาจก่อให้เกิดอันตรายแก่ประโยชน์แห่งรัฐ หัวหน้าหน่วยงานของรัฐมีอำนาจสั่งทำลายได้ หากพิจารณาเห็นว่ามีความจำเป็นอย่างยิ่งที่จะต้องทำลาย

2.8.3 ต้องแต่งตั้ง คณะกรรมการทำลายข้อมูลข่าวสารลับ โดยมีนายทะเบียนข้อมูลข่าวสารลับเป็นประธาน และกรรมการอีกไม่น้อยกว่า 2 คน ซึ่งเป็นเจ้าหน้าที่ที่เกี่ยวข้อง และได้รับความไว้วางใจไม่ต่ำกว่าชั้นความลับของข้อมูลข่าวสารลับนั้น

2.8.4 จัดทำใบรับรองการทำลายข้อมูลข่าวสารลับ โดยนายทะเบียนข้อมูลข่าวสารลับต้องเก็บไว้เป็นหลักฐานไม่น้อยกว่า 1 ปี

2.8.5 เมื่อทำลายข้อมูลข่าวสารลับแล้ว ให้นายทะเบียนข้อมูลข่าวสารลับ จดแจ้งในทะเบียนควบคุมข้อมูลข่าวสารลับด้วย

2.9 หากข้อมูลข่าวสารลับสูญหาย ให้ผู้ทราบข้อเท็จจริงรายงานให้หัวหน้าหน่วยงานของรัฐ ผู้ที่ได้รับมอบหมายที่ตนสังกัดทราบ เพื่อดำเนินการแต่งตั้งคณะกรรมการสอบสวน และให้นายทะเบียนข้อมูลข่าวสารลับบันทึกการสูญหายของข้อมูลข่าวสารลับลงในทะเบียนควบคุมข้อมูลข่าวสารลับ

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

การเปิดเผยข้อมูลข่าวสารลับ

1) การเปิดเผยข้อมูลข่าวสารลับแก่ผู้ใดต้องกระทำโดยระมัดระวัง ในกรณีจำเป็นให้กำหนดเงื่อนไขในการปฏิบัติให้เหมาะสม

2) ข้อมูลข่าวสารลับที่คณะกรรมการวินิจฉัยการเปิดเผยข้อมูลข่าวสารมีคำวินิจฉัยให้เปิดเผย โดยไม่มีข้อจำกัดหรือเงื่อนไขใด ให้ถือว่าข้อมูลข่าวสารลับนั้นถูกยกเลิกชั้นความลับแล้ว เว้นแต่มีการฟ้องคดีต่อศาลและศาลมีคำสั่งหรือคำพิพากษาเป็นอย่างอื่น

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

4) ตามพระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ.2540 มาตรา 37 วรรค 2 คำวินิจฉัยของคณะกรรมการวินิจฉัยการเปิดเผยข้อมูลข่าวสารให้เป็นที่สุด มติ ครม. เมื่อ 11 เม.ย.49 “ห้ามมิให้หน่วยงาน

ของรัฐฟ้องคดีปกครองเพื่อเพิกถอนคำวินิจฉัยของคณะกรรมการวินิจฉัยการเปิดเผยข้อมูลข่าวสารที่มีคำวินิจฉัยให้หน่วยงานของรัฐเปิดเผยข้อมูลข่าวสารแก่ผู้อุทธรณ์”

5) กรณีที่ข้อมูลข่าวสารลับใดไม่มีเครื่องหมายแสดงชั้นความลับ เจ้าหน้าที่ที่เกี่ยวข้องสามารถเปิดเผยข้อมูลข่าวสารลับได้ เว้นแต่เจ้าหน้าที่นั้นได้รู้ หรือควรรู้ว่าข้อมูลข่าวสารนั้นได้มีการกำหนดชั้นความลับไว้

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

3. มาตรฐานการรักษาความปลอดภัยเกี่ยวกับข้อมูลข่าวสารลับทางระบบอิเล็กทรอนิกส์

เพื่อเป็นการคุ้มครองข้อมูลข่าวสารลับทางระบบอิเล็กทรอนิกส์ ไม่ให้สูญหาย ถูกทำลาย เปลี่ยนแปลง หรือรั่วไหล มีความมั่นคงปลอดภัยและเชื่อถือได้ หน่วยงานของรัฐควรพิจารณาถึงหลักการในการรักษาความปลอดภัย เกี่ยวกับข้อมูลข่าวสารลับทางอิเล็กทรอนิกส์ ดังนี้

1. การควบคุมการเข้าถึงกำหนดตัวบุคคล การรหัส จำกัดสิทธิของเจ้าหน้าที่ผู้ใช้งาน ทบทวนสิทธิการเข้าถึงของผู้ใช้งาน และกำหนดพื้นที่ที่มีการรักษาความปลอดภัย

2. การดำเนินการเกี่ยวกับข้อมูลข่าวสารลับทางอิเล็กทรอนิกส์

2.1 การจัดทำ

2.1.1 การจัดทำต้องดำเนินการโดยเจ้าหน้าที่ผู้มีสิทธิในการเข้าถึงข้อมูลข่าวสารลับ และผ่านการตรวจสอบประวัติและพฤติการณ์

2.1.2 ชุดอุปกรณ์คอมพิวเตอร์ที่ใช้จัดทำข้อมูลข่าวสารลับ ไม่ควรใช้เครื่องที่เชื่อมต่อกับระบบเครือข่ายอิเล็กทรอนิกส์ (อินเตอร์เน็ต)

2.1.3 สถานที่ที่ใช้จัดทำข้อมูลข่าวสารลับทางระบบอิเล็กทรอนิกส์ ควรเป็นพื้นที่ที่มีการรักษาความปลอดภัย

2.1.4 การสำเนา การแปล การแจกจ่าย การโอน ข้อมูลข่าวสารลับทางอิเล็กทรอนิกส์ ต้องมีการควบคุมการดำเนินการ

2.2 การจัดเก็บ

2.2.1 ข้อมูลข่าวสารลับทางระบบอิเล็กทรอนิกส์ทุกชั้นความลับ ต้องเข้ารหัส และจัดเก็บในเครื่องคอมพิวเตอร์แม่ข่ายหรือจัดเก็บในสื่ออิเล็กทรอนิกส์ที่มีระบบการรักษาความปลอดภัยในการเข้าใช้งานเครื่องคอมพิวเตอร์

2.2.2 สถานที่จัดเก็บเครื่องคอมพิวเตอร์แม่ข่าย และสื่ออิเล็กทรอนิกส์ควรเป็นพื้นที่ที่มีการรักษาความปลอดภัย

2.2.3 ควรมีระบบสำรองข้อมูลข่าวสารลับทางระบบอิเล็กทรอนิกส์ และเครื่องคอมพิวเตอร์แม่ข่ายสำรอง โดยแยกจัดเก็บในสถานที่ปลอดภัย

2.3 การ รับ-ส่ง

2.3.1 ข้อมูลข่าวสารลับที่ รับ-ส่ง ทางระบบโทรคมนาคม จะต้องดำเนินการเข้ารหัสแล้วเท่านั้น

2.3.2 กำหนดระเบียบปฏิบัติการ รับ-ส่ง ข้อมูลข่าวสารลับทางระบบโทรคมนาคม

2.3.3 จัดทำทะเบียนเจ้าหน้าที่ควบคุมการรหัสและเจ้าหน้าที่การรหัส

2.4 การทำลาย

2.4.1 ขั้นตอนการขออนุมัติทำลายข้อมูลข่าวสารลับทางระบบอิเล็กทรอนิกส์ ใช้หลักการเดียวกับข้อมูลข่าวสารลับที่เป็นเอกสาร

2.4.2 วิธีการทำลายข้อมูลข่าวสารลับทางระบบอิเล็กทรอนิกส์ ใช้ชุดคำสั่งในระบบปฏิบัติการหรือโปรแกรมซึ่งทำหน้าที่ลบแฟ้มข้อมูลโดยไม่สามารถกู้กลับคืนได้

2.3.4 การปฏิบัติตามมาตรฐานการรักษาความปลอดภัยเกี่ยวกับข้อมูลข่าวสารลับทางระบบอิเล็กทรอนิกส์

1. หัวหน้าหน่วยงานของรัฐ อาจมอบหมายให้มีผู้รับผิดชอบ

1.1 ด้านการรักษาความปลอดภัยทางระบบอิเล็กทรอนิกส์ มีหน้าที่ควบคุม กำกับดูแล ตรวจสอบ ให้คำแนะนำ ปรึกษา

1.2 ด้านการบริหารจัดการทางระบบอิเล็กทรอนิกส์ มีหน้าที่กำหนดผู้ใช้ และสิทธิการเข้าถึงข้อมูลข่าวสารลับทางระบบอิเล็กทรอนิกส์

2. การดำเนินการเกี่ยวกับข้อมูลข่าวสารลับทางระบบอิเล็กทรอนิกส์

2.1 การจัดทำ

2.1.1 เจ้าหน้าที่ผู้จัดทำข้อมูลข่าวสารลับทางระบบอิเล็กทรอนิกส์ต้องผ่านการตรวจสอบประวัติและพฤติการณ์ เพื่อรับรองความไว้วางใจก่อนปฏิบัติหน้าที่

2.2.2 สถานที่ที่ใช้จัดทำข้อมูลข่าวสารลับทางระบบอิเล็กทรอนิกส์ กำหนดพื้นที่ให้เป็นพื้นที่หวงห้ามเด็ดขาด หรือหวงห้ามเฉพาะ

2.2.3 การแสดงชั้นความลับของข้อมูลข่าวสารลับทางระบบอิเล็กทรอนิกส์

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

2) หรือใช้กระบวนการทางคอมพิวเตอร์ให้ปรากฏชั้นความลับ เมื่อเรียกแฟ้มข้อมูลมาแสดงภาพ เช่น การจัดทำลายน้ำบนข้อมูลข่าวสารลับทางระบบอิเล็กทรอนิกส์

2.2 การจัดเก็บ

2.2.1 ข้อมูลข่าวสารลับทางอิเล็กทรอนิกส์ทุกชั้นความลับ ต้องเข้ารหัสด้วยเครื่องเข้ารหัสหรือโปรแกรมเข้ารหัส หากใช้โปรแกรมเข้ารหัส ข้อมูลข่าวสารลับทางระบบอิเล็กทรอนิกส์ต้องดำเนินการเข้ารหัสด้วยโปรแกรมเข้ารหัส ซึ่งปัจจุบันมี 2 ประเภทหลักคือ

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

2) กุญแจรหัสแบบอสมมาตร (Asymmetric Key) หรือ ระบบกุญแจคู่ ที่กำหนดให้ใช้กุญแจสองตัว โดยกุญแจตัวหนึ่งใช้ในการเข้ารหัส (Public Key) และกุญแจอีกตัวหนึ่งใช้ในการถอดรหัส (Private Key) นอกจากนี้ยังสามารถประยุกต์ใช้กับการลงลายมือชื่ออิเล็กทรอนิกส์ เพื่อพิสูจน์ความเป็นเจ้าของ และตรวจสอบว่าเป็นข้อมูลข่าวสารลับที่มาจากผู้ส่งนั้นหรือไม่ การใช้กุญแจรหัสประเภทใดและจำนวนครั้งของการเข้ารหัสขึ้นอยู่กับความสำคัญของข้อมูลข่าวสารลับทางระบบอิเล็กทรอนิกส์ ให้อยู่ในดุลพินิจของเจ้าของข้อมูลข่าวสารลับ และหัวหน้าหน่วยงานของรัฐ

2.2.2 สถานที่ที่ใช้จัดทำข้อมูลข่าวสารลับทางระบบอิเล็กทรอนิกส์ กำหนดพื้นที่ให้เป็นพื้นที่หวงห้ามเด็ดขาด หรือหวงห้ามเฉพาะ ห้ามมิให้ผู้ไม่มีอำนาจหน้าที่เกี่ยวข้องเข้าไปในพื้นที่ดังกล่าวโดยไม่ได้รับอนุญาต

2.2.3 ต้องมีระบบสำรองข้อมูลข่าวสารลับทางระบบอิเล็กทรอนิกส์ และเครื่องคอมพิวเตอร์แม่ข่ายสำรอง โดยแยกจัดเก็บในสถานที่ปลอดภัย เพื่อให้ข้อมูลข่าวสารลับทางอิเล็กทรอนิกส์ดำเนินการได้อย่างต่อเนื่อง และความคงอยู่ของข้อมูลข่าวสารลับทางอิเล็กทรอนิกส์ จึงควรมีการสำรองข้อมูลข่าวสารลับดังกล่าวโดยแยกสถานที่จัดเก็บไว้คนละแห่งกับข้อมูลข่าวสารลับทางระบบอิเล็กทรอนิกส์ต้นฉบับ และเพื่อให้การใช้ข้อมูลข่าวสารลับทางระบบอิเล็กทรอนิกส์ได้อย่างต่อเนื่อง ควรมีเครื่องคอมพิวเตอร์แม่ข่ายสำรอง โดยแยกสถานที่จัดเก็บไว้คนละแห่งกับเครื่องคอมพิวเตอร์แม่ข่ายที่ใช้งาน

2.3 การรับ-ส่ง

2.3.1 กำหนดระเบียบปฏิบัติการรับ-ส่ง ข้อมูลข่าวสารลับทาง โทรคมนาคม เช่น

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

2) จัดทำทะเบียนควบคุมการแจกจ่ายกุญแจรหัส เพื่อให้ทราบว่าบุคคลหรือหน่วยงานใดได้รับกุญแจรหัสชุดใด และมีกำหนดระยะเวลาการใช้งาน

3) กำหนดบุคคลรับผิดชอบในการสร้างกุญแจรหัส ซึ่งมิใช่บุคคลเดียวกันกับบุคคลที่จัดทำทะเบียนควบคุม และแจกจ่ายกุญแจรหัส โดยบุคคลดังกล่าวต้องได้รับมอบหมายจากหัวหน้าหน่วยงานของรัฐ

4) จะต้องมีการเปลี่ยนกุญแจรหัสตามห้วงเวลาและสถานการณ์โดยไม่เป็นรูปแบบ และไม่ควรเก็บกุญแจรหัส ไว้ในเครื่องคอมพิวเตอร์ ควรจัดเก็บในสื่ออิเล็กทรอนิกส์ภายนอกอื่น เช่น แผนดิสก์ ซีดีรอม Flash Drive เป็นต้น

5) จะต้องมีการสำรองโปรแกรม และกุญแจรหัส ไม่น้อยกว่า 2 ชุด โดยแยกจัดเก็บรักษาไว้ในสถานที่ปลอดภัย ซึ่งควรเป็นสถานที่คนละแห่ง

6) จัดเครื่องคอมพิวเตอร์โดยเฉพาะในการเข้ารหัส และมีระบบการรักษาความปลอดภัยในการเข้าใช้งานเครื่องคอมพิวเตอร์

2.3.2 จัดทำทะเบียนเจ้าหน้าที่ควบคุมการรหัส และเจ้าหน้าที่การรหัส โดยบุคคลดังกล่าวมีหน้าที่ความรับผิดชอบ ดังนี้

หน้าที่ของเจ้าหน้าที่ควบคุมการรหัสดำเนินการทางการรหัสของหน่วยงาน ภายใต้การกำกับดูแลของ เจ้าหน้าที่ด้านการรักษาความปลอดภัยทางระบบอิเล็กทรอนิกส์ มีหน้าที่ความรับผิดชอบดังนี้

1. ควบคุมเจ้าหน้าที่ผู้เกี่ยวข้องกับการรหัสของหน่วยงาน ว่าเป็นบุคคลที่ได้รับรองความไว้วางใจ และควรผ่านการอบรมด้านการรักษาความปลอดภัยเกี่ยวกับการรักษาความปลอดภัยเกี่ยวกับข้อมูลข่าวสารลับทางระบบอิเล็กทรอนิกส์ แล้ว

2. จัดทำทะเบียนรายชื่อเจ้าหน้าที่การรหัส และมอบหมายหน้าที่เฉพาะส่วน

3. พิจารณาใช้ระบบการรหัสให้เหมาะสมกับชั้นความลับของข้อมูลข่าวสารลับทางอิเล็กทรอนิกส์ และควบคุมการใช้ระบบการรหัสให้ถูกต้อง

4. หากพบการละเมิดการรักษาความปลอดภัยเกี่ยวกับข้อมูลข่าวสารลับทางระบบอิเล็กทรอนิกส์ ให้รายงานหัวหน้าหน่วยงานของรัฐ หรือเจ้าหน้าที่ด้านการรักษาความปลอดภัยทางระบบอิเล็กทรอนิกส์ทันที

หน้าที่ของเจ้าหน้าที่การรหัสรับผิดชอบในการเข้า และถอดการรหัสของหน่วยงานภายใต้การอำนวยการ ควบคุม และกำกับดูแล ของเจ้าหน้าที่ควบคุมการรหัส โดยปฏิบัติ ดังนี้

1. ข้อมูลข่าวสารลับทางระบบอิเล็กทรอนิกส์ ที่จะเข้าการรหัส ต้องผ่านการพิจารณาจาก เจ้าหน้าที่ควบคุมการรหัสก่อน

2. ห้ามเปิดเผยข้อมูลเกี่ยวกับการเข้า หรือถอดรหัส แก่ผู้ที่ไม่มีหน้าที่เกี่ยวข้อง และต้องพิทักษ์รักษาข้อมูลเกี่ยวกับการรหัสให้ปลอดภัยตลอดเวลา

3. หากพบ หรือสงสัยว่ามีละเมิดการรักษาความปลอดภัย ให้รายงานต่อเจ้าหน้าที่ควบคุมการรหัส ทันที

2.3.3 ให้เจ้าหน้าที่ควบคุมการรักษาความปลอดภัยของหน่วยงาน ติดตามผลการปฏิบัติงานเพื่อตรวจสอบการใช้งาน และการละเมิดการรักษาความปลอดภัย

2.4 การทำลาย วิธีการทำลายข้อมูลข่าวสารลับทางระบบอิเล็กทรอนิกส์ กรณีที่ข้อมูลจัดเก็บอยู่ในสื่ออิเล็กทรอนิกส์ เช่น แผ่นดิสก์ ฮาร์ดดิสก์ Flash Drive ที่สามารถใช้บันทึกซ้ำได้ ให้ใช้ชุดคำสั่งในระบบปฏิบัติการหรือโปรแกรมซึ่งทำหน้าที่ลบแฟ้มข้อมูลโดยไม่สามารถกู้กลับคืนได้ กรณีที่จัดเก็บอยู่ในสื่อที่ไม่สามารถใช้บันทึกซ้ำได้ ให้ใช้การทำลายด้วยวิธีทุบ ทำลายให้สิ้นสภาพการใช้งาน

2.4 การรักษาความปลอดภัยเกี่ยวกับสถานที่

การรักษาความปลอดภัยเกี่ยวกับสถานที่ คือ มาตรฐานที่กำหนดขึ้นเพื่อพิทักษ์รักษาให้ความปลอดภัยแก่ที่สงวน อาคาร และสถานที่ของหน่วยงานของรัฐ ตลอดจนวัสดุอุปกรณ์ เจ้าหน้าที่ของรัฐ และข้อมูลข่าวสารในอาคารสถานที่ดังกล่าวให้พ้นจากการโจรกรรม การจารกรรม การก่อวินาศกรรม การก่อการร้าย หรือเหตุอื่นใด อันอาจทำให้เสียสมรรถภาพในการปฏิบัติภารกิจของหน่วยงาน ซึ่งจะส่งผลให้เกิดความเสียหายต่อหน่วยงานของรัฐ

หน่วยงานของรัฐต้องดำเนินการสำรวจ ตรวจสอบ และจัดทำแผนการรักษาความปลอดภัยเกี่ยวกับสถานที่ การกำหนดมาตรฐานการรักษาความปลอดภัยเกี่ยวกับสถานที่ ให้ดำเนินการ ดังนี้

1. หน่วยงานของรัฐต้องกำหนดพื้นที่รักษาความปลอดภัยตามความเหมาะสม กำหนดขอบเขตที่แน่ชัดว่าพื้นที่ใดเป็นพื้นที่ควบคุม หรือพื้นที่หวงห้าม เพื่อควบคุมการเข้า-ออก ของบุคคล และยานพาหนะ

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

3. การควบคุมบุคคลและยานพาหนะ

3.1 การควบคุมบุคคล เพื่อตรวจสอบให้ทราบว่าเป็นบุคคลที่ได้รับอนุญาตให้ผ่านเข้าพื้นที่ โดยจัดทำบัตรผ่าน บัตรแสดงตน และบันทึกหลักฐานการผ่าน เข้า ออก นั้น

3.2 การควบคุมยานพาหนะ เพื่อให้ทราบว่ายานพาหนะใดได้รับอนุญาตให้ผ่านเข้าในบริเวณพื้นที่ได้ และยังรวมถึงการควบคุมบุคคล และสิ่งของต่าง ๆ บนยานพาหนะด้วย

4. ระบบรักษาการณ์ หน่วยงานของรัฐต้องจัดให้มีเจ้าหน้าที่รักษาความปลอดภัยประจำวัน เจ้าหน้าที่ยามรักษาการณ์ วางระบบการติดต่อสื่อสารและสัญญาณแจ้งภัยสำหรับตรวจและเตือนให้ทราบเมื่อ

มีภัย รวมถึงการติดตั้งอุปกรณ์เสริมมาตรการรักษาความปลอดภัยทางเครื่องมือเครื่องใช้อิเล็กทรอนิกส์หรืออื่น ๆ เพื่อให้การรักษาความปลอดภัยมีประสิทธิภาพมากยิ่งขึ้น

5. ระบบป้องกันและระงับอัคคีภัย หัวหน้าหน่วยงานของรัฐต้องจัดให้มีมาตรการป้องกันและระงับอัคคีภัยที่มีประสิทธิภาพ

2.4.1 การปฏิบัติตามมาตรฐานการรักษาความปลอดภัยเกี่ยวกับสถานที่

อาคารสถานที่ ทรัพย์สินมีค่าของแผ่นดินและความลับของทางราชการ รวมถึงบุคคลสำคัญของหน่วยงาน อาจเป็นเป้าหมายของการโจรกรรม การจารกรรม การก่อวินาศกรรม และการก่อการร้ายได้ ดังนั้นจึงจำเป็นต้องวางมาตรการการรักษาความปลอดภัยเกี่ยวกับสถานที่ เพื่อพิทักษ์รักษาบุคคลและทรัพย์สินของทางราชการให้ปลอดภัย หรือขัดขวาง หน่วงเหนี่ยวการดำเนินการของฝ่ายตรงข้ามมิให้สัมฤทธิ์ผล หรือมีผลเสียหายต่อหน่วยงานน้อยที่สุด และยังต้องประสานสอดคล้องกับมาตรการป้องกันภัยทางธรรมชาติ รวมถึงอุบัติภัยด้วย ดังนั้นหน่วยงานของรัฐต้องกำหนดแผนการรักษาความปลอดภัยเกี่ยวกับสถานที่ของหน่วยงานตนเอง โดยสำรวจการรักษาความปลอดภัยเกี่ยวกับสถานที่ของหน่วยงานก่อน จากนั้นจึงนำผลจากการสำรวจเป็นข้อมูลพื้นฐานประกอบในการกำหนดแผน ซึ่งแผนดังกล่าวนี้เป็นเรื่องที่ต้องปฏิบัติเป็นกิจวัตร หน่วยงานเจ้าของแผนจึงต้องพิจารณาปรับปรุง แก้ไขแผนให้มีประสิทธิภาพอยู่ตลอดเวลาการกำหนดมาตรการการรักษาความปลอดภัยเกี่ยวกับสถานที่ ต้องคำนึงถึงหลักการดังนี้

1. กำหนดพื้นที่ที่มีการรักษาความปลอดภัยการกำหนดพื้นที่ที่มีการรักษาความปลอดภัย เพื่อเป็นการป้องกันผู้ไม่มีอำนาจหน้าที่ หรือผู้ไม่ประสงค์ดี เข้าไปในพื้นที่ โดยดำเนินการดังนี้ ต้องมีการเฝ้าตรวจ ผู้ที่จะเข้ามาในพื้นที่ ต้องมีการพิสูจน์ทราบว่าผู้ที่จะเข้ามาเป็นใคร มีวัตถุประสงค์ใด มีสิทธิ มีอำนาจหน้าที่หรือไม่ เป็นภัยหรือไม่ ต้องมีการขัดขวาง หากผู้ที่จะเข้ามาในพื้นที่เป็นผู้ที่ไม่มีอำนาจหน้าที่หรืออาจเป็นภัยได้ พื้นที่หรือบริเวณของส่วนราชการต่าง ๆ ควรกำหนดขอบเขตให้ชัดเจนว่าพื้นที่ใดควรได้รับการรักษาความปลอดภัยเป็นพิเศษ โดยแบ่งพื้นที่ ดังนี้

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

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

2.1 “เขตหวงห้ามเฉพาะ” คือ พื้นที่ซึ่งมีความลับ และบุคคลสำคัญ ต้องมีการตรวจสอบบุคคลที่เข้าถึงอย่างเข้มงวด

2.2 “เขตหวงห้ามเด็ดขาด” คือ พื้นที่ซึ่งมีความลับ และบุคคลที่สำคัญยิ่ง บุคคลที่ได้รับอนุญาตให้เข้าไปใน “เขตหวงห้ามเด็ดขาด” ต้องได้รับการไว้วางใจตามชั้นความลับที่เหมาะสม และใช้มาตรการเสริมเพิ่มเติม เช่น บัตรผ่านเข้า-ออก จะต้องใช้เฉพาะการผ่านเพียงครั้งเดียว และมีการบันทึกการ เข้า-ออก ทุกครั้ง

2. การวางระบบป้องกันทางด้านวัตถุเป็นมาตรการหน่วงเหนี่ยว จำกัด ขัดขวางการรุกล้ำ หรือป้องปราม เพื่อให้เจ้าหน้าที่รักษาความปลอดภัยมีโอกาสตรวจสอบ พิสูจน์ทราบ และขัดขวาง หากมีการบุกรุก การป้องกันทางวัตถุอาจประกอบด้วย

2.1 เครื่องกีดขวางโดยรอบ แบ่งได้เป็น

1) เครื่องกีดขวางตามธรรมชาติ เช่น แม่น้ำ ลำคลอง เป็นต้น อาจพิจารณาดัดแปลง หรือปรับปรุงให้ใช้ประโยชน์เป็นเครื่องกีดขวางได้

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

2.2 การให้แสงสว่างเพื่อให้มาตรการรักษาความปลอดภัยสถานที่มีประสิทธิภาพ การให้แสงสว่าง เพื่อจะให้มองเห็นบริเวณรั้วและเขตหวงห้ามต่าง ๆ โดยชัดเจนในเวลามืด จะได้มองเห็นผู้ที่บุกรุกเข้ามาในสถานที่

3. ระบบการติดต่อสื่อสารและระบบสัญญาณแจ้งภัยระบบการติดต่อสื่อสารและสัญญาณแจ้งภัยจะช่วยให้การติดต่ออำนวยการ ควบคุมสถานการณ์ ตลอดจนรายงานผลการดำเนินการ เป็นไปได้อย่างรวดเร็วทันต่อเหตุการณ์ และมีประสิทธิภาพระบบการติดต่อสื่อสาร เช่นโทรศัพท์ วิทยุสื่อสาร เป็นต้น ต้องสามารถติดต่อ เจ้าหน้าที่ ผู้บังคับบัญชา เพื่อรายงานเหตุการณ์ รวมทั้งติดต่อหน่วยงานอื่น เพื่อระงับยับยั้ง และบรรเทาเหตุที่เกิดขึ้น ระบบสัญญาณแจ้งภัย เช่น เครื่องมือทางอิเล็กทรอนิกส์ ไฟฟ้า เครื่องกล เป็นต้น ที่ทำให้เกิดสัญญาณเมื่อมีผู้บุกรุก หรือเกิดเหตุอื่น ๆ เช่น สัญญาณจับควัน สัญญาณจับคลื่นความร้อน เป็นต้น

4. การควบคุมบุคคลและยานพาหนะเป็นภารกิจหลักของการรักษาความปลอดภัยสถานที่ ผู้รับผิดชอบต้องตรวจสอบบุคคล และยานพาหนะอย่างละเอียด รอบคอบ ถี่ถ้วน เพื่อให้แน่ใจว่าผู้ที่ผ่านเข้ามาในพื้นที่มีสิทธิที่จะผ่านเข้ามาและไม่ก่อเหตุละเมิดการรักษาความปลอดภัย

การควบคุมบุคคล บัตรผ่านและป้ายแสดงตน เป็นหลักฐานแสดงสถานะต่อเจ้าหน้าที่รักษาการณ์ขณะผ่านจุดตรวจ หรือช่องทาง เข้า-ออก ทั้งนี้ถือเป็นการแสดงว่ามีสิทธิในการผ่าน เข้า-ออก และการเข้าถึงพื้นที่ที่มีการรักษาความปลอดภัยได้

บัตรผ่าน คือ บัตรที่หน่วยงานของรัฐออกให้สำหรับบุคคล และยานพาหนะของผู้ที่ปฏิบัติงานอยู่ในพื้นที่นั้น และบุคคลภายนอกที่ต้องเข้ามาติดต่อเป็นการชั่วคราว โดยให้เจ้าหน้าที่รักษาการณ์ทำการบันทึกหลักฐาน ตรวจสอบ และมอบบัตรผ่าน ให้ใช้ในการผ่านเข้า-ออกในแต่ละครั้ง

ป้ายแสดงตน คือ หลักฐานใช้ควบคุมบุคคล ใช้สำหรับบุคคลทั้งภายในและภายนอก เพื่อแสดงสถานะในการเข้าในพื้นที่ที่มีการรักษาความปลอดภัย ป้ายแสดงตน ต้องแสดงไว้ให้เห็นเด่นชัดตลอดเวลาที่อยู่ในพื้นที่

-36-

บันทึกหลักฐานการผ่านเข้า-ออก เป็นมาตรการควบคุมเสริมจากการใช้บัตรผ่าน หรือบัตรแสดงตน โดยจัดให้มีเจ้าหน้าที่บันทึกหลักฐาน สำหรับบุคคลที่ผ่านเข้า-ออก ในพื้นที่ที่มีการรักษาความปลอดภัย โดยให้มีการจดบันทึกรายละเอียดเช่นกัน ส่วนบุคคล ภายนอกในกรณีผู้มาประชุม ติดต่อราชการ หรือพบปะเจ้าหน้าที่ของหน่วยงาน โดยให้มีรายละเอียด เช่น ชื่อ ที่อยู่ของผู้ที่ผ่านเข้า-ออก หน่วยงานที่สังกัด วัน เวลา ที่ผ่านเข้า-ออก ชื่อผู้ที่มาติดต่อ เหตุผลในการผ่าน เข้า-ออก พื้นที่

การควบคุมยานพาหนะ หมายรวมถึง การควบคุมทั้งบุคคล และสิ่งของต่าง ๆ บนยานพาหนะด้วย ยานพาหนะที่ได้รับการอนุญาตให้ผ่านเข้าไปในพื้นที่ ควรกำหนดเส้นทางและที่จอดรถทั้งของเจ้าหน้าที่ภายในและบุคคลภายนอกให้ชัดเจน

การบันทึกหลักฐานยานพาหนะที่ เข้า-ออก ควรมีรายละเอียดดังต่อไปนี้

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

5. ระบบการรักษาการณ์

5.1 ระบบการรักษาการณ์ คือ การจัดและกำหนดเจ้าหน้าที่รักษาความปลอดภัย เจ้าหน้าที่เวรรักษาความปลอดภัยประจำวัน นายตรวจเวร เจ้าหน้าที่รักษาการณ์และหรือยามรักษาการณ์ ปฏิบัติหน้าที่รักษาความปลอดภัยสถานที่ตามห้วงระยะเวลาที่กำหนด และให้รู้จักการใช้เครื่องมืออุปกรณ์ที่เสริมประสิทธิภาพในการปฏิบัติงาน ตลอดจนสนใจข่าวสารที่อาจส่งผลกระทบเป็นภัยต่อหน่วยงาน

5.2 กำลังและขีดความสามารถของเจ้าหน้าที่รักษาการณ์และหรือยาม- รักษาการณ์ เพียงพอกับการปฏิบัติหน้าที่ตามความสำคัญของสถานที่ของส่วนราชการนั้น ๆ หรือไม่ มีการแก้ไขทดแทน หรือปรับปรุงจุดอ่อนเกี่ยวกับเรื่องนี้ด้วยวิธีใด มีการประสานแผนการรักษาความปลอดภัยกับส่วนราชการอื่นที่เกี่ยวข้องหรือไม่

5.3 ต้องมีการคัดเลือก ตรวจสอบประวัติและพฤติการณ์ เพื่อสรรหาตัวบุคคลที่ทำหน้าที่เจ้าหน้าที่รักษาการณ์และหรือยามรักษาการณ์ โดยพิจารณาจากคุณสมบัติด้านคุณธรรม จริยธรรม และสมรรถนะทางร่างกาย

5.4 ต้องมีการกำกับดูแล โดยเจ้าหน้าที่รักษาความปลอดภัยของหน่วยงาน
นั้น ๆ ด้วยวิธีการดังต่อไปนี้

5.4.1 การกำกับดูแลโดยบุคคล หมายถึงการตรวจการปฏิบัติงาน โดยหัวหน้าเจ้าหน้าที่รักษาการณ์ตามลำดับชั้น การตรวจจะทำตั้งแต่ก่อนเริ่มปฏิบัติหน้าที่ ตรวจสภาพทั่วไปของเครื่องมือ อุปกรณ์ อาวุธ ทบทวนคำสั่ง และระเบียบของสถานที่นั้น ตรวจตามระยะเวลาระหว่างการปฏิบัติหน้าที่ เพื่อดูความพร้อม ความเคร่งครัด ความตื่นตัวในการปฏิบัติหน้าที่

5.4.2 การกำกับดูแลโดยเครื่องมือ เป็นการใช้เครื่องมือ หรือวิธีการที่เสมือนบังคับให้เจ้าหน้าที่รักษาการณ์ต้องปฏิบัติตามระยะเวลาที่ทำหน้าที่ เครื่องมือและวิธีการมีดังนี้

1) บันทึกการปฏิบัติ โดยใช้แบบฟอร์มรายงานการปฏิบัติ ให้เจ้าหน้าที่รักษาการณ์เป็นผู้ลงบันทึก ตามจุด และเวลาที่กำหนดไว้

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

5.5 ต้องมีการฝึกอบรมและพัฒนาเจ้าหน้าที่รักษาการณ์และหรือยามรักษาการณ์ เพื่อให้การปฏิบัติหน้าที่มีประสิทธิภาพ ให้ตระหนักถึงภยันตรายที่อาจเกิดขึ้นแก่หน่วยงานสร้างจิตสำนึกในการรักษาความปลอดภัย ฝึก ทบทวน การใช้เครื่องมือ อาวุธ อุปกรณ์ต่าง ๆ ตลอดจนทดสอบความสามารถ วินัยในการปฏิบัติหน้าที่

6. การป้องกันและระงับอัคคีภัย หัวหน้าส่วนราชการต้องกำหนดแผนป้องกันและระงับอัคคีภัย โดยมีเจ้าหน้าที่ควบคุมการรักษาความปลอดภัยของหน่วยงาน เป็นผู้กำหนดรายละเอียดและกำกับดูแลให้เป็นไปตามกฎหมายเกี่ยวกับการป้องกันและระงับอัคคีภัย ในแต่ละหน่วยงานควรพิจารณาดังนี้

6.1 เจ้าหน้าที่ดับเพลิง ควรกำหนดตัวบุคคล และหน้าที่ความรับผิดชอบให้ชัดเจน

6.1.1 ในเวลาราชการ ให้แบ่งกลุ่มเจ้าหน้าที่รับผิดชอบด้านต่าง ๆ เช่น กลุ่มที่ทำหน้าที่ดับเพลิง กลุ่มที่ทำหน้าที่ขนย้ายเอกสารและวัสดุอุปกรณ์ต่าง ๆ กลุ่มที่ทำหน้าที่ค้นหา ตรวจตราผู้ที่หลงเหลือในอาคาร เป็นต้น

6.1.2 นอกเวลาราชการ เป็นหน้าที่ของ เจ้าหน้าที่รักษาความปลอดภัย และเจ้าหน้าที่รักษาการณ์และหรือยามรักษาการณ์ประจำวันที่หน่วยงานกำหนดขึ้นเป็นรับผิดชอบ

6.2 การจัดเตรียมอุปกรณ์ในการดับเพลิง

6.2.1 สัญญาณแจ้งเหตุเพลิงไหม้

6.2.2 เครื่องมือดับเพลิงชั้นต้น เช่น น้ำ ทราย ถัง เชือก ขวาน เป็นต้น อุปกรณ์ถังเคมีดับเพลิงที่เหมาะสมกับเพลิงไหม้ทุกประเภท

6.2.3 ตำแหน่งที่ติดตั้งควรอยู่ในตำแหน่งที่มองเห็นได้ชัดเจน และสามารถนำไปใช้ได้สะดวก

6.2.4 ตรวจสอบอุปกรณ์ทุกชนิดให้อยู่ในสภาพที่ใช้งานได้

6.2.5 หมายเลขโทรศัพท์ของหน่วยงานดับเพลิงที่ติดต่อได้สะดวกรวดเร็ว

6.3 การฝึกอบรมเรื่องการดับเพลิง ให้จัดทำแผนป้องกันและระงับอัคคีภัย เส้นทางหนีไฟ และอบรมให้เจ้าหน้าที่ทุกคนในหน่วยงานระมัดระวังป้องกันการเกิดอัคคีภัย ฝึกซ้อมให้มีความรู้ ความชำนาญในการดับเพลิงเบื้องต้น การหนีไฟตามแผน โดยเจ้าหน้าที่ควรมีความรู้ในเรื่องต่าง ๆ ดังนี้

6.3.1 ประเภทของเพลิง เช่น จากวัสดุธรรมดา น้ำมัน วัตถุเคมี กระแสไฟฟ้าลัดวงจร เป็นต้น

6.3.2 เครื่องมืออุปกรณ์ที่ใช้ในการดับเพลิง ตำแหน่งที่ตั้งวิธีการใช้

6.3.3 การติดต่อสื่อสาร แจ้งเหตุ แผนผังอาคาร เส้นทางเคลื่อนย้าย เส้นทางหนีไฟ 6.3.4 หมายเลขโทรศัพท์หน่วยดับเพลิง

7. อุปกรณ์เสริมมาตรการรักษาความปลอดภัย การติดตั้งอุปกรณ์เสริมมาตรการรักษาความปลอดภัยหน่วยงานของรัฐควรพิจารณาตามความเหมาะสม เช่น ระบบกล้องโทรทัศน์วงจรปิด ซึ่งควรมีผู้รับผิดชอบในการควบคุม เฝ้าดู และตรวจสอบให้อยู่ในสภาพใช้งานได้ตลอดเวลา เป็นต้น

5. มาตรฐานการรักษาความปลอดภัยในการประชุมลับ

หัวหน้าหน่วยงานของรัฐต้องจัดให้มีมาตรการรักษาความปลอดภัยในการประชุมลับ โดยกำหนดมาตรการรักษาความปลอดภัยเกี่ยวกับบุคคล ข้อมูลข่าวสารลับ และสถานที่ เพื่อพิทักษ์รักษาสิ่งที่เป็นความลับของทางราชการที่ปรากฏในการประชุมลับไม่ให้มีการรั่วไหล ถูกจารกรรม รบกวน หรือขัดขวางการประชุม รวมทั้งคุ้มครองบุคคลและสถานที่ที่เกี่ยวข้องกับการประชุมลับนั้นจากการก่อวินาศกรรม ทั้งนี้ ให้นำมาตรฐานของการรักษาความปลอดภัยแต่ละเรื่องมาปรับใช้โดยอนุโลม

2.4.2 การปฏิบัติตามมาตรฐานการรักษาความปลอดภัยในการประชุมลับ

1. หัวหน้าหน่วยงานของรัฐเจ้าของเรื่องที่จะมีการประชุมลับเป็นผู้รับผิดชอบการรักษาความปลอดภัยเกี่ยวกับการประชุมลับนั้น หรืออาจมอบหมายให้บุคคลที่เหมาะสมเป็นผู้ดำเนินการแทนได้ โดยแต่งตั้งเจ้าหน้าที่ควบคุมการรักษาความปลอดภัยในการประชุมลับ และนายทะเบียนข้อมูลข่าวสารลับ รวมทั้งแจ้งให้ผู้เข้าร่วมการประชุมและผู้มีหน้าที่เกี่ยวข้อง ทุกฝ่ายทราบ

2. กรณีการประชุมลับหลายหน่วยงาน ต้องกำหนดหน่วยงานเจ้าภาพรับผิดชอบและแต่งตั้งเจ้าหน้าที่ควบคุมการรักษาความปลอดภัยในการประชุมลับ ทำหน้าที่ประสานงานในเรื่องการรักษาความปลอดภัยกับเจ้าหน้าที่รักษาความปลอดภัยในการประชุมลับของแต่ละหน่วยงาน ซึ่งจะต้องวางมาตรการการรักษาความปลอดภัยเฉพาะในฝ่ายตน ให้สอดคล้องกับมาตรการการรักษาความปลอดภัยในการประชุมลับ

3. การรักษาความปลอดภัยในการประชุมลับต้องคำนึงถึงหลักการดังต่อไปนี้

3.1 บุคคลที่เกี่ยวข้องกับการประชุมลับ ต้องผ่านการตรวจสอบประวัติและพฤติการณ์บุคคลพร้อมทั้งได้รับความไว้วางใจให้เข้าถึงความลับในการประชุมนั้น และ การปฏิบัติงานให้อยู่ในความควบคุมของเจ้าหน้าที่ควบคุมการรักษาความปลอดภัยใน การประชุมลับนั้น สำหรับผู้ที่ไม่มีอำนาจหน้าที่ ต้องไม่ได้รับทราบหรือครอบครองสิ่งที่เป็นความลับของทางราชการในการประชุม

3.2 ห้ามนำเครื่องมือสื่อสาร วัสดุอุปกรณ์ หรือเครื่องบันทึกภาพหรือเสียงเข้าไปในสถานที่ประชุม และต้องไม่นำเครื่องมือ วัสดุอุปกรณ์ หรือข้อมูลข่าวสารใด ๆ ออกนอกสถานที่ประชุมนั้น

4. การรักษาความปลอดภัยในการประชุมลับ ให้หน่วยงานของรัฐพิจารณาดำเนินการดังต่อไปนี้

4.1 กำหนดพื้นที่ที่มีการรักษาความปลอดภัยประกอบด้วยสิ่งดังต่อไปนี้

4.1.1 กำหนดอาณาเขตที่ใช้ในการประชุมลับ ที่ทำการของผู้เข้าประชุมลับ และสถานที่ที่ใช้เก็บรักษาสิ่งที่เป็นความลับของทางราชการ และจัดให้มีมาตรการการรักษาความปลอดภัยตามความจำเป็นและเหมาะสมไว้ล่วงหน้าก่อนเปิดการประชุมลับ

4.1.2 กำหนดให้มีบัตรผ่านหรือป้ายแสดงตนสำหรับใช้ควบคุมบุคคลหลักเกณฑ์และวิธีปฏิบัติในการกำหนดพื้นที่ที่มีการรักษาความปลอดภัย ในการประชุมลับตามวรรคหนึ่ง ให้ดำเนินการตามมาตรการการรักษาความปลอดภัยเกี่ยวกับสถานที่

4.2 ดำเนินการรักษาความปลอดภัย เจ้าหน้าที่ควบคุมการรักษาความปลอดภัยในการประชุมลับต้องดำเนินการดังต่อไปนี้

4.2.1 ตรวจตราและตรวจสอบทางเทคนิคตลอดในพื้นที่ที่กำหนดให้มีการรักษาความปลอดภัยทั้งหมดอย่างละเอียดก่อนวันเปิดประชุมลับและระหว่างการประชุมลับ

4.2.2 ในกรณีที่การประชุมลับนั้นมีความสำคัญมาก หน่วยของรัฐอาจขอความช่วยเหลือจากองค์การรักษาความปลอดภัยได้ หลังจากที่องค์การรักษาความปลอดภัยตรวจสอบแล้ว ให้ส่งมอบความรับผิดชอบในพื้นที่นั้นเป็นลายลักษณ์อักษรแก่เจ้าหน้าที่ควบคุมการรักษาความปลอดภัยในการประชุมลับหรือผู้แทนหน่วยงานนั้น

การปฏิบัติต่อสิ่งที่เป็นความลับของทางราชการ การควบคุม ดูแลการประชุมลับการทำลายข้อมูลข่าวสารลับที่ไม่ใช้แล้ว ให้อยู่ในความดูแลของเจ้าหน้าที่ควบคุมการรักษาความปลอดภัยในการประชุมลับและนายทะเบียนข้อมูลข่าวสารลับ

4.3 ประสานงานการรักษาความปลอดภัย กรณีการประชุมลับหลายหน่วยงานของกำหนดหน่วยงานเจ้าภาพรับผิดชอบและแต่งตั้งเจ้าหน้าที่ควบคุมการรักษาความปลอดภัยในการประชุมลับ โดยผู้เข้าประชุมแต่ละฝ่ายจำเป็นต้องวางมาตรการการรักษาความปลอดภัยเฉพาะในฝ่ายตน ซึ่งการวางมาตรการดังกล่าวต้องสอดคล้องกับมาตรการการรักษาความปลอดภัยในการประชุมลับ ทั้งนี้ เจ้าหน้าที่รักษาความปลอดภัยการ

ประชุมลับ ทำหน้าที่ประสานงานในเรื่องการรักษาความปลอดภัยกับเจ้าหน้าที่ควบคุมการรักษาความปลอดภัยในการประชุมลับ

4.4 กำหนดวิธีปฏิบัติต่อผู้มาติดต่อ หลักเกณฑ์การปฏิบัติต่อผู้มาติดต่อในการประชุมลับ ให้ดำเนินการตามมาตรการการรักษาความปลอดภัยเกี่ยวกับสถานที่ โดยผู้ติดต่อกับผู้เข้าร่วมประชุมลับต้องเป็นบุคคลที่ได้รับอนุญาตให้ผ่านเข้าพื้นที่ที่มีการรักษาความปลอดภัย พื้นที่ควบคุม หรือพื้นที่หวงห้าม และกำหนดให้มีบัตรผ่านหรือป้ายแสดงตนสำหรับใช้ควบคุมบุคคล รวมทั้งจัดให้มีการบันทึกหลักฐานสำหรับผู้มาติดต่อ ทั้งนี้ จัดให้มีสถานที่พักรอสำหรับผู้มาติดต่อ

4.5 แถลงข่าวต่อสื่อมวลชน กรณีจำเป็นต้องมีการแถลงข่าวเกี่ยวกับการประชุมลับ ให้ผู้รับผิดชอบจัดประชุมดำเนินการดังต่อไปนี้

4.5.1 จัดสถานที่ที่ใช้แถลงข่าวขึ้นโดยเฉพาะ และควรอยู่นอกพื้นที่ที่มีการรักษาความปลอดภัยในการประชุมลับ

4.5.2 กำหนดให้ผู้แถลงข่าว หัวข้อที่จะนำแถลง และข้อมูลข่าวสารที่จะเผยแพร่ ต้องได้รับอนุมัติจากที่ประชุมลับก่อน หรือในกรณีที่ที่ประชุมลับมอบหมายให้มีผู้แถลงข่าวหลายคน ผู้แถลงข่าวแต่ละคนต้องแถลงเฉพาะเรื่องที่ตนได้รับอนุมัติจากที่ประชุมลับเท่านั้น

4.5.3 ควบคุมให้การแถลงข่าวหรือการเผยแพร่ข้อมูลข่าวสารและผู้เข้ารับฟังเป็นไปด้วยความเหมาะสม

4.6 บรรยายหรือบรรยายสรุปเรื่องที่เป็นความลับ ในกรณีที่เป็นการบรรยายหรือการบรรยายสรุปเรื่องที่เป็นความลับ นอกจากจะต้องปฏิบัติตามมาตรการในการรักษาความปลอดภัยในการประชุมลับแล้ว ให้ดำเนินการดังต่อไปนี้

4.6.1 กำหนดชั้นความลับของการบรรยายหรือการบรรยายสรุปโดยถือตามชั้นความลับที่สูงสุดในข้อมูลข่าวสาร หรือสิ่งที่ใช้ประกอบการบรรยายหรือการบรรยายสรุปนั้น

4.6.2 กำหนดให้ผู้เข้ารับฟังทุกคนต้องได้รับความไว้วางใจให้เข้าถึงชั้นความลับของการบรรยายหรือการบรรยายสรุปนั้น

4.6.3 เมื่อเริ่มและสิ้นสุดการบรรยายหรือการบรรยายสรุปผู้บรรยายต้องแจ้งให้ผู้เข้ารับฟังรับทราบชั้นความลับของการบรรยาย และเน้นย้ำให้ดำเนินการรักษาความปลอดภัยต่อสิ่งที่ได้รับฟังจากการบรรยายหรือการบรรยายสรุปนั้น

6. มาตรฐานการปฏิบัติเมื่อเกิดการละเมิดการรักษาความปลอดภัย

หัวหน้าหน่วยงานของรัฐต้องกำหนดแนวทางปฏิบัติ เมื่อเกิดการละเมิดการรักษาความปลอดภัย เพื่อลดระดับความเสียหายกรณีเกิดการละเมิด ฝ่าฝืน หรือละเลยไม่ปฏิบัติตามมาตรการรักษาความปลอดภัยที่กำหนดไว้ จะโดยเจตนาหรือไม่ก็ตาม อันเป็นเหตุให้ความลับของทางราชการรั่วไหล หรือเป็นเหตุให้เจ้าหน้าที่ของรัฐ วัสดุอุปกรณ์ ทรัพย์สินของรัฐได้รับความเสียหาย และป้องกันไม่ให้เกิดซ้ำ ค้นหาข้อบกพร่อง สาเหตุ เพื่อนำมาปรับปรุงแก้ไขมาตรการรักษาความปลอดภัยให้รัดกุมยิ่งขึ้น

2.4.3 การปฏิบัติเมื่อเกิดการละเมิดการรักษาความปลอดภัย

1. ให้เจ้าหน้าที่ของรัฐผู้พบเห็นหรือทราบ หรือสงสัยว่าจะมีหรือมีการละเมิดมาตรการการรักษาความปลอดภัย รีบดำเนินการเบื้องต้นเพื่อลดความเสียหายให้เหลือ น้อยที่สุดและรายงานผู้บังคับบัญชา หรือเจ้าหน้าที่ควบคุมการรักษาความปลอดภัย หรือเจ้าหน้าที่ผู้รับผิดชอบ หรือแจ้งเจ้าของเรื่องเดิมทราบโดยเร็วที่สุด

2. ให้เจ้าหน้าที่ควบคุมการรักษาความปลอดภัยหรือเจ้าหน้าที่ผู้รับผิดชอบ ดำเนินการดังต่อไปนี้

2.1 สำรวจและตรวจสอบความเสียหายอันเกิดจากการละเมิดมาตรการการรักษาความปลอดภัย

2.2 ดำเนินการเพื่อป้องกันหรือลดความเสียหายให้เหลือน้อยที่สุด

2.3 สำรวจตรวจสอบและค้นหาสาเหตุแห่งการละเมิดมาตรการการรักษา ความปลอดภัย ตลอดจนจุดอ่อนและข้อบกพร่องต่าง ๆ

2.4 ดำเนินการแก้ไขมาตรการการรักษาความปลอดภัยให้รัดกุมยิ่งขึ้น เพื่อป้องกันมิให้มีการละเมิดมาตรการการรักษาความปลอดภัยเกิดขึ้นอีก

2.5 รายงานรายละเอียดเกี่ยวกับการละเมิดมาตรการการรักษาความปลอดภัยต่อผู้บังคับบัญชาตามลำดับชั้น หากมีข้อมูลข่าวสารลับสูญหายให้รายงานและบันทึกลงในทะเบียนควบคุมข้อมูลข่าวสารลับด้วย

2.6 หากปรากฏหลักฐานหรือข้อสงสัยว่าเกิดการจารกรรม หรือการก่อวินาศกรรม ให้รายงานและขออนุมัติผู้บังคับบัญชาตามลำดับชั้น เพื่อแจ้งเรื่องให้เจ้าหน้าที่ผู้มีอำนาจหน้าที่ในด้านการสืบสวนดำเนินการต่อไป

3. เมื่อได้ดำเนินการตามข้อ 2 แล้ว ให้หัวหน้าหน่วยงานของรัฐ ดำเนินการดังต่อไปนี้

3.1 แจ้งให้หน่วยงานของรัฐซึ่งเป็นเจ้าของเรื่องเดิมหรือเจ้าของสถานที่หรือผู้ที่เกี่ยวข้องทราบทันที

3.2 สอบสวนเพื่อให้ทราบว่าผู้ใดเป็นผู้ละเมิดและผู้ใดเป็นผู้รับผิดชอบต่อ การละเมิดนั้น

3.3 พิจารณาแก้ไขข้อบกพร่องและป้องกันมิให้เหตุการณ์เช่นนั้นเกิดขึ้น ซ้ำอีก

3.4 พิจารณาดำเนินการลงโทษตามกฎหมายต่อผู้ละเมิดมาตรการการรักษาความปลอดภัย หรือผู้จะละเมิด และผู้รับผิดชอบต่อการละเมิดนั้น

4. ให้หน่วยงานของรัฐซึ่งเป็นเจ้าของเรื่องเดิมหรือผู้ที่เกี่ยวข้อง ดำเนินการดังต่อไปนี้

4.1 พิจารณาว่าสมควรลดหรือยกเลิกชั้นความลับของสิ่งที่เป็นความลับของทางราชการนั้นหรือไม่

4.2 ขจัดความเสียหายอันเกิดจากการละเมิดมาตรการการรักษาความปลอดภัยที่จะมีต่อความมั่นคงและผลประโยชน์แห่งรัฐ ในการนี้ อาจต้องเปลี่ยนนโยบายและแผน พร้อมทั้งปัจจัยต่าง ๆ ที่เกี่ยวข้องตามที่เห็นสมควร

บทที่ 3
ระเบียบวิธีวิจัย

3.1 ประชากรและกลุ่มตัวอย่าง

การวิจัยครั้งนี้เป็นการวิจัยเชิงคุณภาพศึกษาจากเอกสารที่เกี่ยวข้องและทำการเก็บรวมรวบข้อมูลจากการสนทนากลุ่มผู้เชี่ยวชาญด้านการรักษาความปลอดภัยทั้งภาครัฐและเอกชนที่ทำงานทั้งในระดับนโยบายและระดับปฏิบัติการ โดยใช้วิธีการเลือกผู้เข้าร่วมสนทนากลุ่มแบบเฉพาะเจาะจงจำนวน 10 คน แต่มีผู้ตอบรับเข้าร่วมการสนทนากลุ่มจำนวนทั้งสิ้น 8 คน

3.2 วิธีการดำเนินการวิจัย

การดำเนินการวิจัยเป็นการวิจัยเชิงคุณภาพ โดยมีขั้นตอนดังนี้

ขั้นตอนที่ 1 ศึกษาเอกสาร ตำรา และงานวิจัยที่เกี่ยวข้องกับเรื่องของมาตรการทางด้านการรักษาความปลอดภัย

ขั้นตอนที่ 2 การสนทนากลุ่มกับกลุ่มผู้บริหารและเจ้าหน้าที่รักษาความปลอดภัยทั้งของหน่วยงานภาครัฐและเอกชนเพื่อกำหนดแนวทางในการสร้างกรอบและข้อคำถามเพื่อนำไปสู่การพัฒนาเกณฑ์ประเมินมาตรการทางด้านการรักษาความปลอดภัย

ขั้นตอนที่ 3 นำข้อมูลที่ได้จากขั้นตอนที่ 1-2 โดยการหาข้อสรุปของตัวชี้วัดจากการทำเทคนิคการวิเคราะห์เนื้อหา (Content Analysis) เพื่อนำไปสู่การกำหนดเกณฑ์ชี้วัด

ขั้นตอนที่ 4 สร้างเกณฑ์การประเมินมาตรการทางด้านการรักษาความปลอดภัยสำหรับองค์การภาครัฐ

3.3 วิธีการวิเคราะห์ข้อมูล

การวิเคราะห์ข้อมูลสำหรับงานวิจัยในครั้งนี้ประกอบด้วย 1) การวิเคราะห์ข้อมูลจากเอกสาร (Documentary Analysis) โดยการสังเคราะห์เนื้อหา ประเด็น และองค์ประกอบที่เกี่ยวข้องกับเรื่องการกำหนดแนวทางการรักษาความปลอดภัยในองค์การ แล้วนำมาจัดกลุ่มให้สอดคล้องกัน และ 2) การวิเคราะห์ข้อมูลจากการสนทนากลุ่ม โดยข้อมูลที่ได้จากการบันทึกเสียงและการบันทึกด้วยลายมือจากประเด็นคำถามที่ได้กำหนดขึ้น ซึ่งได้มาจากการทบทวนวรรณกรรมและสังเคราะห์เพื่อนำไปกำหนดประเด็นข้อคำถาม จำนวนทั้งหมด 6 ข้อ ประกอบด้วย

- ให้ท่านนิยามคำว่าการรักษาความปลอดภัยตามความเข้าใจของท่าน

- ปัญหาของการรักษาความปลอดภัยในหน่วยงานภาคเอกชนที่ท่านพบ มีประเด็นใดบ้าง
- ถ้าพิจารณาถึงองค์การที่มีมาตรการการรักษาความปลอดภัยทางกายภาพที่เป็นเลิศ หรือมีการปฏิบัติที่ดีเยี่ยม ท่านนึกถึงองค์การใดทั้งภาครัฐและเอกชน อะไรเป็นปัจจัยสำคัญที่ท่านพิจารณาองค์การนั้นเป็นองค์การแห่งความเป็นเลิศด้านความปลอดภัย
- เมื่อพิจารณาถึงจุดแข็งและจุดอ่อนเกี่ยวกับมาตรการการรักษาความปลอดภัยของหน่วยงานของท่านเอง ท่านคิดว่ามีประเด็นใดบ้างที่สามารถนำมาแลกเปลี่ยนในครั้งนี้ได้ อะไรเป็นสิ่งที่ท่านคิดว่าควรเติมเต็มหรือเป็นประเด็นที่ยังทำได้ไม่ครบถ้วน
- ถ้าพิจารณาองค์ประกอบของระบบการรักษาความปลอดภัยทางกายภาพ ท่านคิดว่ามีองค์ประกอบใดบ้างที่สำคัญต่อเกี่ยวข้องกับระบบการรักษาความปลอดภัยทางกายภาพ
- โดยปกติหน่วยงานของท่านมีการประเมินมาตรการด้านการรักษาความปลอดภัยภายในหน่วยงานของท่านอยู่เป็นประจำหรือไม่ ท่านดำเนินการประเมินอย่างไร และนำแนวทางมาใช้ในการปรับปรุงอย่างไรบ้าง

โดยคณะผู้วิจัยได้ทำการวิเคราะห์เนื้อหา (Content Analysis) ของข้อมูลที่ได้จากการสนทนากลุ่มเพื่อสกัดประเด็นที่เกี่ยวข้องหรือเชื่อมโยงกับเรื่องมาตรการการรักษาความปลอดภัย และเมื่อได้ประเด็นหรือปัจจัยที่เกี่ยวข้องแล้ว ทางคณะผู้วิจัยได้นำเอาปัจจัยหรือประเด็นต่างๆ เหล่านั้นไปเชื่อมโยงด้วยวิธีการหาความสัมพันธ์กับปัจจัยที่ได้จากการวิเคราะห์จากเอกสารที่เกี่ยวข้อง นำไปสู่การกำหนดประเด็นที่เกี่ยวข้องกับมาตรการด้านการรักษาความปลอดภัย

บทที่ 4
ผลการวิเคราะห์ข้อมูล

งานวิจัยเรื่องการพัฒนาเกณฑ์การประเมินมาตรการด้านการรักษาความปลอดภัยสำหรับหน่วยงานภาคเอกชนได้ดำเนินการวิเคราะห์ข้อมูลผ่านการวิเคราะห์จากเอกสารและการทำสนทนากลุ่ม ได้ผลดังนี้

4.1 ผลการวิจัย

1) ผลการวิจัยจากการวิเคราะห์เอกสาร

ขั้นตอนแรกของการวิจัยเรื่องการพัฒนาเกณฑ์การประเมินมาตรการด้านการรักษาความปลอดภัยสำหรับหน่วยงานเอกชน ได้ทำการวิเคราะห์เอกสารที่เกี่ยวข้องกับเรื่องการรักษาความปลอดภัย โดยใช้คำสำคัญในการสืบค้นข้อมูล ได้แก่ “ความมั่นคงปลอดภัย” “ความปลอดภัยทางกายภาพ” “องค์ประกอบของการรักษาความปลอดภัย” และ “การประเมินการรักษาความปลอดภัย” ซึ่งมีเอกสารที่เกี่ยวข้องกับเรื่องการรักษาความปลอดภัยที่กล่าวถึงองค์ประกอบของงานรักษาความปลอดภัย ดังนี้

1.1) ข้อมูลเกี่ยวกับองค์ประกอบด้านความมั่นคงปลอดภัยทางกายภาพที่สำคัญ จาก บริษัท RETA Security, Inc. โดยข้อมูลของบริษัท RETA Security ชี้ให้เห็นว่าสิ่งที่องค์การต้องให้ความสำคัญเพื่อการรักษาความปลอดภัยและปกป้องทรัพย์สินขององค์การ ที่ครอบคลุมถึง ชีวิตของบุคคลที่เกี่ยวข้องกับองค์การทั้งหมด อาคารและพื้นที่ขององค์การ และอุปกรณ์และสิ่งของต่างๆ ขององค์การ ประกอบด้วยสิ่งต่างๆ ดังต่อไปนี้

- การเตรียมความพร้อมต่อสถานการณ์ฉุกเฉิน เช่น อุปกรณ์ที่ใช้ในสถานการณ์ฉุกเฉิน แนวปฏิบัติเมื่ออยู่ในสถานการณ์วิกฤติหรือฉุกเฉิน (Crisis and Emergency Flip Chart) การซ้อมรับมือในสถานการณ์ฉุกเฉิน
- การเพิ่มประสิทธิภาพการสื่อสาร เช่น โทรศัพท์ที่มีการติดแนบหมายเลขฉุกเฉินที่สำคัญไว้ทุกเครื่อง ระบบอินเตอร์คอม วิทยุสื่อสารแบบสองทาง และโทรศัพท์เคลื่อนที่
- การรักษาความปลอดภัยในส่วนทางเข้าหรือประตูทางเข้าอาคาร เช่นระบบจดจำใบหน้าของบุคคลที่เข้าเยี่ยมหรือผู้มาติดต่อ ระบบควบคุมการเข้าอาคาร (การกำหนดพื้นที่ในการเข้าถึง) รวมถึงกระจกนิรภัยที่สามารถป้องกันกระสุนได้

- การมีส่วนร่วมของพนักงาน เช่น การสร้างแนวทางในการระแวดระวังร่วมกันของพนักงาน การสร้างชุมชนแห่งความปลอดภัย และการฝึกอบรมและให้รางวัลแก่พนักงานที่ปฏิบัติตามระเบียบและรวมถึง
- ระบบกล้องวงจรปิด ที่สามารถตรวจความเคลื่อนไหวได้และเชื่อมต่อกับระบบโทรศัพท์มือถือ

นอกจากนี้บริษัท RETA Security, Inc. ยังชี้ให้เห็นถึงองค์ประกอบที่สำคัญที่ใช้สำหรับการประเมินการรักษาความปลอดภัยขององค์การประกอบด้วย 5 ส่วนที่สำคัญ ได้แก่

- แผนการบริหารความเสี่ยง
- การบริหาร/ การจัดการของผู้บริหาร
- การรักษาความปลอดภัยอาคาร
- การป้องกันความรุนแรง
- การฝึกอบรมพนักงาน

1.2) ข้อมูลการรักษาความปลอดภัยทางกายภาพ โดย Brain LeBlanc ที่ให้ข้อมูลเกี่ยวกับการรักษาความปลอดภัยทางกายภาพว่าเป็นการเตรียมการในการปกป้องทรัพย์สิน บุคคล สิ่งอำนวยความสะดวกและวัสดุอุปกรณ์จากการบุกรุก การทำลาย การก่อวินาศกรรม การขโมย และการก่ออาชญากรรมในรูปแบบต่างๆ โดยระบบรักษาความปลอดภัยที่สำคัญประกอบด้วย ระบบรั้ว ระบบแสงไฟ ระบบตรวจจับการบุกรุก (Intrusion Detection System) ระบบกล้องวงจรปิด (CCTV) และระบบการควบคุมการเข้าออก (Access Control) ซึ่งระบบแต่ละประเภทควรถูกจัดการให้เกื้อหนุนซึ่งกันและกัน นอกเหนือจากอุปกรณ์หรือระบบต่างๆ เหล่านี้ องค์ประกอบของการรักษาความปลอดภัย ยังรวมถึง นโยบายและแนวปฏิบัติ (Policies and Procedures) หลักสูตรฝึกอบรม (Training Programs) พนักงานหรือบุคลากร (Employees) และพนักงานรักษาความปลอดภัย (Security Staff) ซึ่งองค์ประกอบและแนวปฏิบัติเหล่านี้ต้องสนับสนุนซึ่งกันและกัน เพื่อนำไปสู่หัวใจสำคัญของภารกิจการรักษาความปลอดภัย ที่ประกอบด้วย การทำถ่วงเวลา (Delay) การตรวจจับ (Detect) และการตอบสนอง (Respond) หมายความว่า องค์ประกอบของการรักษาความปลอดภัยต้องทำให้บุคคลที่ไม่พึงประสงค์ใช้เวลาและความพยายามที่นานพอสมควรในการทำลายระบบรักษาความปลอดภัย และเมื่อบุคคลที่ไม่พึงปรารถนาใช้เวลานานมากขึ้นเท่าใดโอกาสที่จะถูกตรวจจับก็มีมากขึ้นเท่านั้น ซึ่งการถูกตรวจจับอาจเกิดขึ้นจากระบบตรวจจับการบุกรุก (IDS) ระบบกล้องวงจรปิด (CCTV) หรือจากเจ้าหน้าที่รักษา

ความปลอดภัย (Security Officers) และภายหลังจากที่มีการถ่วงเวลาและตรวจจับเกิดขึ้น ขั้นตอนที่สำคัญที่สุดคือการตอบสนอง ซึ่งอาจเกี่ยวข้องกับการแจ้งเจ้าหน้าที่ของรัฐให้เข้ามาตรวจสอบ หรือการเพิ่มความระแวดระวังมากยิ่งขึ้น รวมถึงการปรับเปลี่ยนนโยบายหรือหลักปฏิบัติที่เกี่ยวข้องกับมาตรการรักษาความปลอดภัย อย่างไรก็ตามภารกิจทั้ง 3 ส่วนนี้ต้องทำหน้าที่ในการสอดประสานซึ่งกันและกัน เพราะถ้าปราศจากความสามารถในการการถ่วงเวลา โอกาสที่ตรวจพบบุคคลหรือสิ่งต้องสงสัยก็จะไม่เกิดขึ้น และถ้าปราศจากความสามารถในการตรวจจับ บุคคลที่จะเข้ามาก่อการรู้ว่าตนเองจะไม่ได้รับการตอบโต้ใดๆ จากทางองค์การ และถ้าปราศจากความสามารถในการตอบสนอง บุคคลที่ไม่พึงปรารถนาจะไม่เกิดความเกรงกลัวและพร้อมที่จะดำเนินการเพื่อบรรลุภารกิจของตนในอนาคต

นอกจากนี้ Brian LeBlanc ยังได้ระบุถึงองค์ประกอบพื้นฐานของการรักษาความปลอดภัยไว้ ดังนี้

- การประเมินภัยคุกคาม (Threat Assessment) โดยเริ่มต้นจากขั้นตอนการทำบัญชีกลุ่มหรือบุคคลในเขตพื้นที่ที่สามารถก่ออาชญากรรมหรือทำให้เกิดภัยคุกคามต่อองค์การได้ โดยครอบคลุมเรื่องของวิธีการและกลุ่มเป้าหมายที่กลุ่มบุคคลเหล่านั้นน่าจะเลือกใช้ ขั้นตอนที่สองคือการประเมินภัยคุกคาม โดยการกำหนดลักษณะหรือรูปแบบของภัยคุกคามที่อาจเกิดขึ้น ซึ่งขึ้นอยู่กับคุณลักษณะของสภาพแวดล้อมเป้าหมาย โดยพิจารณาจากความน่าจะเป็นที่กำหนดจากข้อมูลเดิมในอดีต เช่น การแจ้งเหตุกับหน่วยงานราชการ ข้อมูลอาชญากรรม รายงานภายในขององค์การ การสัมภาษณ์พนักงาน ภัยคุกคามที่เกิดขึ้นกับธุรกิจที่คล้ายคลึงกัน และพิจาณาจากผลลัพธ์ของภัยคุกคามว่าจะนำไปสู่เรื่องใดได้บ้าง เช่น การสูญเสียชีวิต ทรัพย์สิน อุปกรณ์ที่สำคัญ หรือทรัพยากรที่สำคัญขององค์การ ขั้นตอนต่อไปคือการประเมินภัยคุกคามเพื่อกำหนดลักษณะและรูปแบบการคุกคามที่ผู้ก่อนการนิยมปฏิบัติ โดยศึกษาจากข้อมูลในอดีตที่ผ่านมา ความสามารถ โอกาส และความตั้งใจ ขั้นตอนต่อไปเป็นการประเมินเป้าหมายเพื่อพิจารณาว่าสิ่งใดที่มีแนวโน้มจะเป็นเป้าหมายที่ถูกคุกคาม เช่นการก่อการเชิงสัญลักษณ์ การทำลายสาธารณูปโภค การทำลายผู้บริสุทธิ์ และการฉวยโอกาส และขั้นตอนสุดท้ายคือความอ่อนแอของเป้าหมายไม่ว่าจะเป็นในส่วนของภาคเอกชนเองหรือการตอบสนองของหน่วยงานความมั่นคงของรัฐ ที่นำไปสู่การระบุถึงช่องว่างทางการข่าวและความต้องการด้านการข่าว

- การสำรวจด้านการรักษาความปลอดภัย (Security Survey) เป็นการประเมินความปลอดภัยของพื้นที่โดยมีการกำหนดวัตถุประสงค์เพื่อกำหนดสภาพการรักษาความปลอดภัยในปัจจุบันขององค์การ และระบุถึงความไม่แน่นอนที่อาจเกิดขึ้น และข้อเสนอแนะเพื่อการปรับปรุงมาตรการการรักษาความปลอดภัยให้ดียิ่งขึ้น
- สิ่งกีดขวาง (Barriers) เป็นการกำหนดขอบเขตหรือปริมณฑลของหน่วยงานที่แสดงให้เห็นถึงการยับยั้งผู้ที่อาจเข้ามาบุกรุกทั้งเชิงกายภาพและทางจิตใจ
- ระบบแสงสว่าง (Lighting)
- ระบบควบคุมการเข้าออก (Access Control)
- ระบบควบคุมการปิดเปิด (Locks and Key Control)
- ระบบการตรวจจับผู้บุกรุก (Intrusion Detection Systems: IDS) ถูกออกแบบมาเพื่อตรวจจับการบุกรุกหรือการเข้าสถานที่โดยไม่ได้รับอนุญาตและระบุถึงพื้นที่ที่ถูกบุกรุกพร้อมทั้งส่งสัญญาณเตือนเมื่อมีการบุกรุก ทำให้เกิดการตรวจตราความปลอดภัยในองค์การได้อย่างต่อเนื่องและครอบคลุมขอบเขตการรักษาความปลอดภัยไปยังพื้นที่ที่เจ้าหน้าที่อาจไม่สามารถเข้าไปได้
- ตู้นิรภัย (Security Containers) ไว้สำหรับปกป้องเอกสารที่สำคัญขององค์การ
- กล้องวงจรปิด (CCTV) ถูกนำมาใช้ในฐานะระบบที่ช่วยให้มองเห็นภาพในมุมที่ลับตาหรือพื้นที่ที่อยู่ไกลออกไป และสามารถนำไปใช่ร่วมกับระบบเตือนภัยอื่นๆ ได้เช่นระบบตรวจจับอุณหภูมิหรือควันไฟที่จะทำให้ระบบกล้องวงจรปิดสามารถยืนยันได้ว่ามีเหตุเพลิงไหม้เกิดขึ้นในพื้นที่ห่างไกลออกไป หรือระบบแจ้งเตือนการบุกรุกในพื้นที่ที่อยู่ไกลออกไปในบริเวณของหน่วยงานสามารถเชื่อมต่อเข้ากับระบบกล้องวงจรปิดได้เช่นเดียวกัน

2) ผลการวิจัยจากการสนทนากลุ่ม

ขั้นตอนที่สองของการวิจัยเรื่องการพัฒนาเกณฑ์การประเมินมาตรการด้านการรักษาความปลอดภัยสำหรับหน่วยงานเอกชน ได้ดำเนินการจัดทำการสนทนากลุ่ม (Focus Group) โดยได้เชิญบุคคลที่มีประสบการณ์เกี่ยวข้องกับงานด้านการรักษาความปลอดภัยทั้งจากหน่วยงานภาครัฐและเอกชน เข้าร่วม

แลกเปลี่ยนประสบการณ์ โดยหัวหน้าคณะผู้วิจัยได้ทำหน้าที่เป็นผู้ดำเนินการสนทนากลุ่มด้วยตนเอง โดยมีรายนามของผู้เข้าร่วมการสนทนากลุ่ม ดังตารางที่ 1

ตารางที่ 1 รายชื่อผู้เข้าร่วมการสนทนากลุ่ม (Focus Group)

ผู้เข้าร่วม	ตำแหน่ง/ หน่วยงาน
1. ร.ต. ศักดา จันทรวงศ์	อดีตเจ้าหน้างานด้านการรักษาความปลอดภัย ธนาคารแห่งประเทศไทย
2. คุณระวิวรรณ พัฒนาจันทร์	เจ้าหน้าที่งานรักษาความปลอดภัย สำนัก 10 สำนักข่าวกรองแห่งชาติ
3. คุณศิริรัตน์ สนธิปัญญา	เจ้าหน้าที่งานรักษาความปลอดภัย สำนัก 10 สำนักข่าวกรองแห่งชาติ
4. คุณกาญจนา งามเนตร	เจ้าหน้าที่งานรักษาความปลอดภัย สำนัก 10 สำนักข่าวกรองแห่งชาติ
5. คุณสาร ศรีบุญเรือง	เจ้าหน้าที่รักษาความปลอดภัย บริษัท รักษาความปลอดภัย เอส. เอส. ซี. ปอนด์ไฟร์ เซฟตี้ จำกัด สำนักงานใหญ่
6. คุณอนุชา ช้างน้อย	ผู้จัดการฝ่ายบริหารการตลาด บริษัทแรงเจอร์อินเวสติเกชั่น จำกัด
7. คุณบุญเรือน ทองทิพย์	กรรมการผู้อำนวยการ บริษัทแรงเจอร์อินเวสติเกชั่น จำกัด
8. คุณเอกชัย ชำนินา	ที่ปรึกษางานรักษาความปลอดภัย บริษัทแรงเจอร์อินเวสติเกชั่น จำกัด

สำหรับประเด็นคำถามที่ใช้สำหรับการดำเนินการสนทนากลุ่ม ประกอบด้วยคำถามดังต่อไปนี้

- ให้ท่านนิยามคำว่าการรักษาความปลอดภัยตามความเข้าใจของท่าน
- ปัญหาของการรักษาความปลอดภัยในหน่วยงานภาคเอกชนที่ท่านพบ มีประเด็นใดบ้าง
- ถ้าพิจารณาถึงองค์การที่มีมาตรการการรักษาความปลอดภัยทางกายภาพที่เป็นเลิศ หรือมีการปฏิบัติที่ดีเยี่ยม ท่านนึกถึงองค์การใดทั้งภาครัฐและเอกชน อะไรเป็นปัจจัยสำคัญที่ท่านพิจารณาองค์การนั้นเป็นองค์การแห่งความเป็นเลิศด้านความปลอดภัย
- เมื่อพิจารณาถึงจุดแข็งและจุดอ่อนเกี่ยวกับมาตรการการรักษาความปลอดภัยของหน่วยงานของท่านเอง ท่านคิดว่ามีประเด็นใดบ้างที่สามารถนำมาแลกเปลี่ยนในครั้งนี้ได้ อะไรเป็นสิ่งที่ท่านคิดว่าควรเติมเต็มหรือเป็นประเด็นที่ยังทำได้ไม่ครบถ้วน
- ถ้าพิจารณาองค์ประกอบของระบบการรักษาความปลอดภัยทางกายภาพ ท่านคิดว่ามีองค์ประกอบใดบ้างที่สำคัญต่อเกี่ยวข้องกับระบบการรักษาความปลอดภัยทางกายภาพ

- โดยปกติหน่วยงานของท่านมีการประเมินมาตรการด้านการรักษาความปลอดภัยภายในหน่วยงานของท่านอยู่เป็นประจำหรือไม่ ท่านดำเนินการประเมินอย่างไร และนำแนวทางมาใช้ในการปรับปรุงอย่างไรบ้าง

สาเหตุสำคัญของการตั้งประเด็นคำถามเกี่ยวกับนิยามการรักษาความปลอดภัยเพื่อสร้างความชัดเจนว่า ผู้เข้าร่วมมีความเข้าใจตรงกันถึงความหมายของคำว่าการรักษาความปลอดภัย ซึ่งจากการสนทนากลุ่มพบว่า ผู้เข้าร่วมมีการให้นิยามที่สอดคล้องไปในทิศทางเดียวกันว่า “การรักษาความปลอดภัยคือการสร้างความปลอดภัยสูงสุดทั้งต่อชีวิตและทรัพย์สิน หรือเป็นกิจกรรมที่ดำเนินการตามมาตรการที่กำหนดไว้เพื่อป้องกันไม่ให้เกิดความเสียหาย แก่บุคคล ข้อมูลสารสนเทศ และสถานที่” ซึ่งถ้าพิจารณาในมิติที่เกี่ยวข้องกับภาคเอกชน ผู้เข้าร่วมการสนทนากลุ่มบางท่านให้คำนิยามการรักษาความปลอดภัยไว้ว่า “เป็นการตอบสนองต่อบุคคลที่ต้องการความปลอดภัยในชีวิตและทรัพย์สิน ที่เจ้าหน้าที่ของรัฐไม่สามารถให้ได้หรือไม่สามารถดูแลได้ทั่วถึง” หรือ “เป็นเรื่องที่ผู้รับจ้างต้องทำให้ผู้ว่าจ้างได้รับความปลอดภัยสูงสุด” โดยสรุปการรักษาความปลอดภัยคือการพิทักษ์รักษาหน่วยงานที่รวมถึงชีวิตและทรัพย์สินโดยการกำหนดมาตรการในการป้องกันเพื่อให้เกิดความปลอดภัยสูงสุด”

ในส่วนของประเด็นที่เกี่ยวกับปัญหาการรักษาความปลอดภัยในหน่วยงานเอกชนที่พบ ทางผู้เข้าร่วมสนทนากลุ่ม ได้ชี้ให้เห็นประเด็นที่สอดคล้องกันเกี่ยวกับปัญหาการรักษาความปลอดภัยในหลากหลายประเด็น ซึ่งสามารถสรุปได้ดังนี้ ปัญหาที่พบโดยส่วนใหญ่คือปัญหาที่ทางองค์การเอกชนได้กำหนดมาตรการรักษาความปลอดภัยขึ้นโดยอาจร่วมมือกับบริษัทที่ปรึกษาด้านการรักษาความปลอดภัย แต่ไม่ได้ทำตามมาตรการที่กำหนดไว้ โดยการดำเนินงานด้านการรักษาความปลอดภัยมีลักษณะของความยืดหยุ่นในระเบียบ ทำให้เกิดความย่อหย่อนซึ่งส่งผลให้การรักษาความปลอดภัยไม่มีประสิทธิภาพและประสิทธิผลเท่าที่ควร โดยยกตัวอย่างของบริษัทน้ำมันของเอกชนรายหนึ่งที่ตนเองได้มีส่วนเกี่ยวข้องกับงานด้านการรักษาความปลอดภัย ที่มีมาตรการเรื่องของการห้ามสูบบุหรี่ การนำไฟแช็ค และการห้ามใส่รองเท้าแตะเข้ามาในบริเวณโรงงาน เมื่อทางพนักงานรักษาความปลอดภัยทำตามมาตรการที่กำหนดไว้อย่างเคร่งครัด กลับถูกผู้มีอำนาจสั่งการให้ผ่อนปรนมาตรการดังกล่าวเนื่องจากบุคคลที่ไม่ทำตามมาตรการด้านการรักษาความปลอดภัยเหล่านั้นเป็นบุคลที่ทำหน้าที่ขนถ่ายน้ำมันจากเรือเข้าโรงงาน ซึ่งถ้าไม่อนุญาตให้บุคคลเหล่านี้เข้าโรงงานก็จะไม่สามารถขนถ่ายน้ำมันได้

นอกจากนี้ผู้เข้าร่วมสนทนากลุ่มบางส่วนเห็นว่าปัญหาของการรักษาความปลอดภัยอยู่ที่ นโยบายของผู้บริหารหรือทัศนคติของผู้บริหารที่มีต่อเรื่องการรักษาความปลอดภัย เช่นเมื่อมีการประชุมหรือการให้ความรู้เกี่ยวกับเรื่องของการรักษาความปลอดภัย ผู้บริหารมักไม่ส่งบุคคลที่เกี่ยวข้องเข้ามาเรียนรู้ จึงทำให้ไม่สามารถทำให้งานด้านการรักษาความปลอดภัยนำไปสู่การปฏิบัติได้ แต่พอเมื่อเกิดปัญหาก็ประสานงานเพื่อขอความช่วยเหลือ นอกจากนี้บุคลากรในองค์การหลายแห่งส่วนใหญ่ไม่ทราบว่าหน่วยงานของตนมีระเบียบหรือมาตรการที่เกี่ยวกับเรื่องการรักษาความปลอดภัย และส่วนใหญ่มักถามว่าถ้าไม่ทำตามมาตรการเหล่านี้จะได้รับบทลงโทษหรือไม่ ในส่วนที่เกี่ยวข้องกับบุคลากร ผู้เข้าร่วมสนทนากลุ่มมองว่าปัญหาเกี่ยวกับการรักษาความปลอดภัยมาจากการขาดจิตสำนึกที่ดีเพียงพอของบุคลากรและผู้บริหาร ต้องรอให้เกิดเหตุการณ์ที่ไม่พึงปรารถนาขึ้นก่อนจึงค่อยเห็นถึงความสำคัญ ในขณะที่เกิดเหตุการณ์ที่ส่งผลกระทบต่อความมั่นคงปลอดภัยขององค์การ หน่วยงานขาดแผนหรือมาตรการในการรับมือกับเหตุการณ์หรืออาจปรับมาตรการและแผนเมื่อเกิดเหตุการณ์ เช่น บางหน่วยงานที่เช่าพื้นที่ภายนอก อาจมองว่าพื้นที่ไม่ใช่ของตนจึงไม่ได้ให้ความสนใจหรือสังเกตการเปลี่ยนแปลงในพื้นที่ของตนเอง

สำหรับผู้เข้าร่วมสนทนากลุ่มที่มาจากบริษัทรักษาความปลอดภัยมองว่า ปัญหาและอุปสรรคของงานด้านการรักษาความปลอดภัยมาจาก 3 ประเด็นที่สำคัญ คือ 1) วัฒนธรรมของสังคมที่ไม่เน้นเรื่องของกฎระเบียบ ข้อบังคับและกติกา โดยมีการหลีกเลี่ยงและไม่ปฏิบัติตามกฎเนื่องจากไม่ชอบให้มีการบังคับ 2) หน่วยงานที่รับหน้าที่ในการทำงานด้านการรักษาความปลอดภัยแก่บริษัทที่ว่าจ้างมักไม่ค่อยให้ความสำคัญกับเนื้องานที่ตนเองทำเท่าที่ควร ไม่ว่าจะเป็นเรื่องของการตรวจสอบภาพรวมของระบบการรักษาความปลอดภัยอย่างสม่ำเสมอ แต่เน้นทำงานแบบทำเป็นประจำไม่เปลี่ยนแปลงรูปแบบ เพราะเนื่องจากว่าเรื่องของการรักษาความปลอดภัยสิ่งใดก็ตามที่ดูเหมือนว่าเป็นปกติแสดงว่าอาจมีความไม่ปกติเกิดขึ้น และ 3) การให้การสนับสนุนจากภาครัฐต่อการทำงานด้านการรักษาความปลอดภัย โดยภาครัฐไม่ได้มองบริษัทเอกชนที่เข้ามาทำงานด้านการรักษาความปลอดภัยในฐานะส่วนหนึ่งของการให้ความช่วยเหลือเจ้าหน้าที่ของรัฐ แต่กลับมองเป็นธุรกิจ เช่น พ.ร.บ. ธุรกิจรักษาความปลอดภัย พ.ศ. 2558 ที่มองว่าเป็นอุปสรรคต่อการทำงานด้านการรักษาความปลอดภัย ซึ่งประเด็นที่ผู้เข้าร่วมสนทนาท่านนี้ได้เสนออาจไม่ได้เกี่ยวข้องกับเรื่องของปัญหาการรักษาความปลอดภัยในองค์การโดยตรง แต่เป็นปัญหาที่เกิดขึ้นกับบริษัทที่ทำธุรกิจรักษาความปลอดภัยมากกว่า อย่างไรก็ดีถ้าเชื่อมโยงความเกี่ยวข้องอาจพิจารณาได้ว่า การที่บริษัทรักษาความปลอดภัยถูกกำหนดข้อบังคับมากมายโดยเฉพาะอย่างยิ่งการกำหนดวุฒิการศึกษา การอบรมพนักงานอาจส่งผลให้บริษัทที่รับจ้าง

ดูแลงานรักษาความปลอดภัยมีบุคลากรไม่เพียงพอต่อการทำหน้าที่เพื่อตอบสนองเรื่องการรักษาวามปลอดภัยแก่ผู้ว่าจ้างได้

นอกจากนี้ผู้เข้าร่วมสนทนากลุ่มที่มาจากบริษัทรักษาความปลอดภัยอีกท่าน ได้ให้ความเห็นว่า ปัญหาด้านการรักษาความปลอดภัยขององค์การในภาพรวมมากจากปัญหาเรื่อง “คน” ทั้งจากตัวบริษัทที่เป็นผู้ว่าจ้าง (ทีมบริหาร) ไม่รับนโยบายเกี่ยวกับงานรักษาความปลอดภัย จากผู้มาติดต่อหรือตัวบุคลากรในองค์การ ที่ไม่เคารพกฎระเบียบข้อบังคับเกี่ยวกับการรักษาความปลอดภัย และจากตัวบริษัทที่รับจ้างทำงานด้านการรักษาความปลอดภัยเอง ที่ไม่ยึดระเบียบของตัวเอง ไม่มีความสม่ำเสมอในการทำงาน และการบริหารบุคลากรที่ไม่ดีเพียงพอ เป็นต้น

ในประเด็นที่สอดคล้องกันกับเรื่อง “คน” ผู้เข้าร่วมการสนทนาบางท่านเห็นว่า ปัญหาเกี่ยวกับการรักษาความปลอดภัยที่เกิดขึ้นในบางครั้งมาจากตัวบุคคลที่อยู่ในองค์การเองที่มีการเปลี่ยนแปลงพฤติกรรม เช่น มีภาระหนี้สินที่เพิ่มมากขึ้น หรือมีรายจ่ายที่เพิ่มมากขึ้น ซึ่งอาจทำให้แสดงพฤติกรรมที่เป็นภัยคุกคามต่อความมั่นคงปลอดภัยชองสมาชิกในองค์การได้

จะเห็นได้ว่า เมื่อมีการกล่าวถึงประเด็นที่เกี่ยวข้องกับเรื่องของงานรักษาความปลอดภัย ผู้เข้าร่วมสนทนากลุ่มที่มาจากบริษัทที่ทำธุรกิจรักษาความปลอดภัย จะให้ความสำคัญของปัญหาที่เชื่อมโยงกับบริษัทที่รับจ้างดูแลงานรักษาความปลอดภัยด้วย ซึ่งในความเป็นจริงแล้วบางบริษัทอาจไม่ได้จ้างบริษัทภายนอกทำหน้าที่ดูแลงานรักษาความปลอดภัยให้แก่บริษัทของตน อย่างไรก็ตามถ้าพิจารณาจากประเด็นที่ผู้เข้าร่วมสนทนาทั้งหมดได้นำเสนอ พบว่า ปัญหาเรื่องการรักษาความปลอดภัยมีพื้นฐานมาจากเรื่องของ “คน” เป็นสำคัญ ทั้งจากผู้บริหาร บุคลากรในองค์การเอง ผู้ที่มาติดต่อกับองค์การ รวมถึงบุคลากรจากหน่วยงานภายนอกที่เข้ามาทำหน้าที่ดูแลงานรักษาความปลอดภัยให้กับองค์การที่เป็นผู้ว่าจ้างด้วย

เมื่อมีการสนทนาประเด็นที่เกี่ยวข้องกับเรื่องขององค์ประกอบของระบบการรักษาความปลอดภัยทางกายภาพ ผู้เข้าร่วมการสนทนากลุ่มได้นำเสนอประเด็นที่น่าสนใจที่สามารถนำมาสรุปเป็นองค์ประกอบเกี่ยวกับงานด้านรักษาความปลอดภัยขององค์การได้ ดังนี้

1) องค์ประกอบที่เกี่ยวกับเรื่องของการนำเทคโนโลยีหรืออุปกรณ์เข้ามาใช้ในการรักษาความปลอดภัยเพื่อการป้องปราม โดยมีการใช้เจ้าหน้าที่ในการควบคุมเทคโนโลยี และเมื่อเกิดเหตุการณ์ที่ไม่พึงประสงค์ขึ้นเจ้าหน้าที่สามารถเข้าระงับเหตุได้อย่างทันท่วงที โดยที่บุคลากรในหน่วยงานต้องทราบว่าองค์การของตนมีอุปกรณ์ที่เกี่ยวข้องกับเรื่องการรักษาความปลอดภัยใดบ้าง และบุคลากรที่ทำหน้าที่ดูแลงานรักษาความ

ปลอดภัยต้องได้รับข้อมูลและฝึกอบรมให้ใช้อุปกรณ์นั้นอย่างถูกต้องอยู่เสมอ โดยผู้เข้าร่วมการสนทนาที่มาจากสำนักข่าวกรองแห่งชาติได้ยกตัวอย่าง เหตุการณ์เพลิงไหม้ที่ห้องเก็บเอกสารธนาคารไทยพาณิชย์สำนักงานใหญ่ เมื่อปี 2558 ที่มีผู้เสียชีวิตหลายรายเนื่องจากระบบดับเพลิงอัตโนมัติที่ถูกติดตั้งอยู่ภายในห้องเก็บเอกสารเป็นระบบเซ็นเซอร์ป้องกันเพลิงไหม้แบบอัตโนมัติ ที่ใช้แก๊สไพโรเจนซึ่งไล่ออกซิเจนในบริเวณที่เกิดเพลิงไหม้ออกไป ส่งผลให้บุคคลที่เข้าไประงับเหตุขาดอากาศหายใจและเสียชีวิตในที่สุด ดังนั้นการใช้อุปกรณ์หรือเทคโนโลยีทั้งหลายต้องมีคนคุมและมีการแจ้งเตือนแก่ผู้ที่เกี่ยวข้อง

2) องค์ประกอบเกี่ยวกับแผนปฏิบัติในสภาวะปกติและสภาวะฉุกเฉิน เช่น ในกรณีที่องค์การตั้งอยู่ในพื้นที่ที่เป็นจุดยุทธศาสตร์ เช่น มหาวิทยาลัยเทคโนโลยีราชมงคลพระนครมีพื้นที่อยู่ติดกับทำเนียบรัฐบาล ความเสี่ยงที่อาจเกิดขึ้นประการหนึ่งคือการชุมนุมประท้วง (ม็อบ) ซึ่งเมื่อเกิดเหตุการณ์ในลักษณะนี้ขึ้นให้ถือว่าองค์การอยู่ในสภาวะที่ไม่ปกติหรือสภาวะฉุกเฉิน ดังนั้นองค์การจึงต้องมีแผนรับมือหรือปฏิบัติการในสภาวะฉุกเฉินด้วย

3) องค์ประกอบเกี่ยวกับการวิเคราะห์และประเมินสภาพแวดล้อม หรือการกำหนดระดับความสำคัญของพื้นที่ (Casing) โดยผู้ที่ทำงานที่เกี่ยวข้องกับงานรักษาความปลอดภัยต้องศึกษาสภาพแวดล้อมโดยรอบขององค์การและวิเคราะห์สิ่งบอกเหตุเพื่อสามารถกำหนดมาตรการและแนวปฏิบัติเพื่อจัดการกับสถานการณ์ที่อาจเกิดขึ้นได้

4) องค์ประกอบเกี่ยวกับการสร้างเครือข่ายระหว่างหน่วยงาน ผู้เข้าร่วมสนทนากลุ่มส่วนใหญ่มองว่าภาคเอกชนขาดเรื่องของการสร้างเครือข่ายระหว่างองค์การที่ช่วยให้เกิดการแลกเปลี่ยนและติดตามความเคลื่อนไหวของปัจจัยที่อาจส่งผลกระทบต้องความมั่นคงปลอดภัยขององค์การได้

5) องค์ประกอบเกี่ยวกับนโยบายเกี่ยวกับงานด้านการรักษาความปลอดภัย ต้องสอดคล้องกับการนำไปปฏิบัติให้เกิดเป็นรูปธรรม ซึ่งในความเป็นจริงสวนทางกัน เนื่องจากว่างานด้านการรักษาความปลอดภัยเป็นเรื่องที่ทำให้เกิดความไม่สะดวกสบาย ดังนั้นอาจมีการลดระดับความเข้มข้นของมาตรการลงตามความรู้สึกหรือความต้องการของบุคคลที่ทำงานในองค์การนั้น ซึ่งไม่ถูกต้องและไม่ได้สะท้อนให้เห็นถึงความใส่ใจต้องมาตรการการรักษาความปลอดภัยอย่างแท้จริง

6) องค์ประกอบเกี่ยวกับกายภาพของมนุษย์ พิจารณาจากสรีระของผู้ที่ทำหน้าที่รักษาความปลอดภัยที่ควรมีรูปร่างสูงใหญ่ กำยำเป็นที่น่าเกรงขามแก่บุคคลที่จะก่อเหตุ

7) องค์ประกอบเกี่ยวกับการฝึกปฏิบัติมาตรการรักษาความปลอดภัยอย่างสม่ำเสมอ

ทั้ง 7 องค์ประกอบนี้เป็นองค์ประกอบที่ผู้เข้าร่วมการสนทนากลุ่มได้นำเสนอและพิจารณาว่ามีความสำคัญต้องระบบการรักษาความปลอดภัยขององค์การและควรถูกนำไปใช้ในการประเมินองค์ประกอบของระบบการรักษาความปลอดภัยสำหรับหน่วยงานเอกชนด้วย

4.2 สรุปเกณฑ์การประเมินมาตรการการรักษาความปลอดภัย

จากการวิเคราะห์เอกสารและผลการสนทนากลุ่มจากบุคคลที่เกี่ยวข้องกับการปฏิบัติงานด้านการรักษาความปลอดภัยทั้งจากหน่วยงานภาครัฐและเอกชน นำไปสู่การกำหนดเกณฑ์การประเมินมาตรการการรักษาความปลอดภัยเพื่อนำไปสู่การประเมินของผู้เชี่ยวชาญในลำดับต่อไปได้ ดังนี้

เกณฑ์การประเมินมาตรการการรักษาความปลอดภัย	**แหล่งที่มาของข้อมูล**	
	การวิเคราะห์เอกสาร	**การสนทนากลุ่ม**
การสร้างความตระหนักรู้เกี่ยวกับการพัฒนาด้านเทคโนโลยีที่เกี่ยวข้องกับการรักษาความปลอดภัย	√	√
การบูรณาการองค์ประกอบทางด้านสถาปัตยกรรม	√	-
ระบบการรักษาความปลอดภัย	√	√
ทรัพยากรมนุษย์	√	√
หลักปฏิบัติด้านการรักษาความปลอดภัย	√	√

เกณฑ์ที่ใช้ในการประเมินต่อความพร้อมของมาตรการรักษาความปลอดภัยขององค์การภาครัฐได้แก่ การสร้างความตระหนักรู้เกี่ยวกับการพัฒนาด้านเทคโนโลยีที่เกี่ยวข้องกับการรักษาความปลอดภัย การเชื่อมโยงองค์ประกอบด้านสถาปัตยกรรม การพัฒนาระบบการรักษาความปลอดภัย การจัดการทรัพยากรมนุษย์ที่ครอบคลุมเจ้าหน้าที่รักษาความปลอดภัยและการให้ความรู้ที่เกี่ยวข้องกับบุคลากรในองค์การ และการกำหนดหลักปฏิบัติด้านการรักษาความปลอดภัยที่สอดคล้องกับธรรมชาติและกายภาพขององค์การ

บทที่ 5
สรุป อภิปรายผล และข้อเสนอแนะ

5.1 สรุป

งานวิจัยเรื่องการพัฒนาเกณฑ์การประเมินมาตรการด้านการรักษาความปลอดภัยสำหรับหน่วยงานภาคเอกชนได้ดำเนินการวิเคราะห์ข้อมูลผ่านการวิเคราะห์จากเอกสารและการทำสนทนากลุ่ม โดยใช้วิธีการเลือกผู้เข้าร่วมสนทนากลุ่มแบบเฉพาะเจาะจงจำนวน 10 คน แต่มีผู้ตอบรับเข้าร่วมการสนทนากลุ่มจำนวนทั้งสิ้น 8 คน โดยมีขั้นตอนการวิจัยทั้งหมด 4 ขั้นตอน ได้แก่ ขั้นตอนที่ 1 ศึกษาเอกสาร ตำรา และงานวิจัยที่เกี่ยวข้องกับเรื่องของมาตรการทางด้านการรักษาความปลอดภัย ขั้นตอนที่ 2 การสนทนากลุ่มกับกลุ่มผู้บริหารและเจ้าหน้าที่รักษาความปลอดภัยทั้งของหน่วยงานภาครัฐและเอกชนเพื่อกำหนดแนวทางในการสร้างกรอบและข้อคำถามเพื่อนำไปสู่การพัฒนาเกณฑ์ประเมินมาตรการทางด้านการรักษาความปลอดภัย ขั้นตอนที่ 3 นำข้อมูลที่ได้จากขั้นตอนที่ 1-2 โดยการหาข้อสรุปของตัวชี้วัดจากการทำเทคนิคการวิเคราะห์เนื้อหา (Content Analysis) เพื่อนำไปสู่การกำหนดเกณฑ์ชี้วัด และขั้นตอนที่ 4 สร้างเกณฑ์การประเมินมาตรการทางด้านการรักษาความปลอดภัยสำหรับองค์การภาครัฐ

ในส่วนของการวิเคราะห์ข้อมูลสำหรับงานวิจัยในครั้งนี้ประกอบด้วย 2 ส่วนที่สำคัญ ได้แก่ 1) การวิเคราะห์ข้อมูลจากเอกสาร (Documentary Analysis) โดยการสังเคราะห์เนื้อหา ประเด็น และองค์ประกอบที่เกี่ยวข้องกับเรื่องการกำหนดแนวทางการรักษาความปลอดภัยในองค์การ แล้วนำมาจัดกลุ่มให้สอดคล้องกัน และ 2) การวิเคราะห์ข้อมูลจากการสนทนากลุ่ม โดยข้อมูลที่ได้จากการบันทึกเสียงและการบันทึกด้วยลายมือจากประเด็นคำถามที่ได้กำหนดขึ้น ซึ่งได้มาจากการทบทวนวรรณกรรมและสังเคราะห์เพื่อนำไปกำหนดประเด็นข้อคำถาม จำนวนทั้งหมด 6 ข้อ ดังนี้

- ให้ท่านนิยามคำว่าการรักษาความปลอดภัยตามความเข้าใจของท่าน
- ปัญหาของการรักษาความปลอดภัยในหน่วยงานภาคเอกชนที่ท่านพบ มีประเด็นใดบ้าง
- ถ้าพิจารณาถึงองค์การที่มีมาตรการการรักษาความปลอดภัยทางกายภาพที่เป็นเลิศ หรือมีการปฏิบัติที่ดีเยี่ยม ท่านนึกถึงองค์การใดทั้งภาครัฐและเอกชน อะไรเป็นปัจจัยสำคัญที่ท่านพิจารณาองค์การนั้นเป็นองค์การแห่งความเป็นเลิศด้านความปลอดภัย

- เมื่อพิจารณาถึงจุดแข็งและจุดอ่อนเกี่ยวกับมาตรการการรักษาความปลอดภัยของหน่วยงานของท่านเอง ท่านคิดว่ามีประเด็นใดบ้างที่สามารถนำมาแลกเปลี่ยนในครั้งนี้ได้ อะไรเป็นสิ่งที่ท่านคิดว่าควรเติมเต็มหรือเป็นประเด็นที่ยังทำได้ไม่ครบถ้วน
- ถ้าพิจารณาองค์ประกอบของระบบการรักษาความปลอดภัยทางกายภาพ ท่านคิดว่ามีองค์ประกอบใดบ้างที่สำคัญต่อเกี่ยวข้องกับระบบการรักษาความปลอดภัยทางกายภาพ
- โดยปกติหน่วยงานของท่านมีการประเมินมาตรการด้านการรักษาความปลอดภัยภายในหน่วยงานของท่านอยู่เป็นประจำหรือไม่ ท่านดำเนินการประเมินอย่างไร และนำแนวทางมาใช้ในการปรับปรุงอย่างไรบ้าง

โดยคณะผู้วิจัยได้ทำการวิเคราะห์เนื้อหา (Content Analysis) ของข้อมูลที่ได้จากการสนทนากลุ่มเพื่อสกัดประเด็นที่เกี่ยวข้องหรือเชื่อมโยงกับเรื่องมาตรการการรักษาความปลอดภัย และเมื่อได้ประเด็นหรือปัจจัยที่เกี่ยวข้องแล้ว ทางคณะผู้วิจัยได้นำเอาปัจจัยหรือประเด็นต่างๆ เหล่านั้นไปเชื่อมโยงด้วยวิธีการหาความสัมพันธ์กับปัจจัยที่ได้จากการวิเคราะห์จากเอกสารที่เกี่ยวข้อง เพื่อนำไปสู่การกำหนดประเด็นที่เกี่ยวข้องกับมาตรการด้านการรักษาความปลอดภัย

5.2 การอภิปรายผล

ผลที่ได้จากการวิเคราะห์เอกสารที่เกี่ยวข้องกับการรักษาความปลอดภัย สามารถสรุปได้ดังนี้

- การประเมินภัยคุกคาม (Threat Assessment) โดยเริ่มต้นจากขั้นตอนการทำบัญชีกลุ่มหรือบุคคลในเขตพื้นที่ที่สามารถก่ออาชญากรรมหรือทำให้เกิดภัยคุกคามต่อองค์การได้ โดยครอบคลุมเรื่องของวิธีการและกลุ่มเป้าหมายที่กลุ่มบุคคลเหล่านั้นน่าจะเลือกใช้ ขั้นตอนที่สองคือการประเมินภัยคุกคาม โดยการกำหนดลักษณะหรือรูปแบบของภัยคุกคามที่อาจเกิดขึ้น ซึ่งขึ้นอยู่กับคุณลักษณะของสภาพแวดล้อมเป้าหมาย โดยพิจารณาจากความน่าจะเป็นที่กำหนดจากข้อมูลเดิมในอดีต เช่น การแจ้งเหตุกับหน่วยงานราชการ ข้อมูลอาชญากรรม รายงานภายในขององค์การ การสัมภาษณ์พนักงาน ภัยคุกคามที่เกิดขึ้นกับธุรกิจที่คล้ายคลึงกัน และพิจาณาจากผลลัพธ์ของภัยคุกคามว่าจะนำไปสู่เรื่องใดได้บ้าง เช่น การสูญเสียชีวิต ทรัพย์สิน อุปกรณ์ที่สำคัญ หรือทรัพยากรที่สำคัญขององค์การ ขั้นตอน

ต่อไปคือการประเมินภัยคุกคามเพื่อกำหนดลักษณะและรูปแบบการคุกคามที่ผู้ก่อนการนิยมปฏิบัติ โดยศึกษาจากข้อมูลในอดีตที่ผ่านมา ความสามารถ โอกาส และความตั้งใจ ขั้นตอนต่อไปเป็นการประเมินเป้าหมายเพื่อพิจารณาว่าสิ่งใดที่มีแนวโน้มจะเป็นเป้าหมายที่ถูกคุกคาม เช่นการก่อการเชิงสัญลักษณ์ การทำลายสาธารณูปโภค การทำลายผู้บริสุทธิ์ และการฉวยโอกาส และขั้นตอนสุดท้ายคือความอ่อนแอของเป้าหมายไม่ว่าจะเป็นในส่วนของภาคเอกชนเองหรือการตอบสนองของหน่วยงานความมั่นคงของรัฐ ที่นำไปสู่การระบุถึงช่องว่างทางการข่าวและความต้องการด้านการข่าว

- การสำรวจด้านการรักษาความปลอดภัย (Security Survey) เป็นการประเมินความปลอดภัยของพื้นที่โดยมีการกำหนดวัตถุประสงค์เพื่อกำหนดสภาพการรักษาความปลอดภัยในปัจจุบันขององค์การ และระบุถึงความไม่แน่นอนที่อาจเกิดขึ้น และข้อเสนอแนะเพื่อการปรับปรุงมาตรการการรักษาความปลอดภัยให้ดียิ่งขึ้น
- สิ่งกีดขวาง (Barriers) เป็นการกำหนดขอบเขตหรือปริมณฑลของหน่วยงานที่แสดงให้เห็นถึงการยับยั้งผู้ที่อาจเข้ามาบุกรุกทั้งเชิงกายภาพและทางจิตใจ
- ระบบแสงสว่าง (Lighting)
- ระบบควบคุมการเข้าออก (Access Control)
- ระบบควบคุมการปิดเปิด (Locks and Key Control)
- ระบบการตรวจจับผู้บุกรุก (Intrusion Detection Systems: IDS) ถูกออกแบบมาเพื่อตรวจจับการบุกรุกหรือการเข้าสถานที่โดยไม่ได้รับอนุญาตและระบุถึงพื้นที่ที่ถูกบุกรุกพร้อมทั้งส่งสัญญาณเตือนเมื่อมีการบุกรุก ทำให้เกิดการตรวจตราความปลอดภัยในองค์การได้อย่างต่อเนื่องและครอบคลุมขอบเขตการรักษาความปลอดภัยไปยังพื้นที่ที่เจ้าหน้าที่อาจไม่สามารถเข้าไปได้
- ตู้นิรภัย (Security Containers) ไว้สำหรับปกป้องเอกสารที่สำคัญขององค์การ
- กล้องวงจรปิด (CCTV) ถูกนำมาใช้ในฐานะระบบที่ช่วยให้มองเห็นภาพในมุมที่ลับตาหรือพื้นที่ที่อยู่ไกลออกไป และสามารถนำไปใช่ร่วมกับระบบเตือนภัยอื่นๆ ได้เช่นระบบตรวจจับอุณหภูมิหรือควันไฟที่จะทำให้ระบบกล้องวงจรปิดสามารถยืนยันได้ว่ามีเหตุเพลิงไหม้เกิดขึ้น

ในพื้นที่ห่างไกลออกไป หรือระบบแจ้งเตือนการบุกรุกในพื้นที่ที่อยู่ไกลออกไปในบริเวณของหน่วยงานสามารถเชื่อมต่อเข้ากับระบบกล้องวงจรปิดได้เช่นเดียวกัน

ผลที่ได้จากการวิเคราะห์การสนทนากลุ่มที่เกี่ยวข้องกับประเด็นการพัฒนามาตรการการรักษาความปลอดภัย สามารถสรุปได้ดังนี้

องค์ประกอบเกี่ยวกับงานด้านรักษาความปลอดภัยขององค์การ ประกอบด้วย 7 องค์ประกอบต่อไปนี้

1) องค์ประกอบที่เกี่ยวกับเรื่องของการนำเทคโนโลยีหรืออุปกรณ์เข้ามาใช้ในการรักษาความปลอดภัยเพื่อการป้องปราม โดยมีการใช้เจ้าหน้าที่ในการควบคุมเทคโนโลยี และเมื่อเกิดเหตุการณ์ที่ไม่พึงประสงค์ขึ้นเจ้าหน้าที่สามารถเข้าระงับเหตุได้อย่างทันท่วงที โดยที่บุคลากรในหน่วยงานต้องทราบว่าองค์การของตนมีอุปกรณ์ที่เกี่ยวข้องกับเรื่องการรักษาความปลอดภัยใดบ้าง และบุคลากรที่ทำหน้าที่ดูแลงานรักษาความปลอดภัยต้องได้รับข้อมูลและฝึกอบรมให้ใช้อุปกรณ์นั้นอย่างถูกต้องอยู่เสมอ โดยผู้เข้าร่วมการสนทนาที่มาจากสำนักข่าวกรองแห่งชาติได้ยกตัวอย่าง เหตุการณ์เพลิงไหม้ที่ห้องเก็บเอกสารธนาคารไทยพาณิชย์สำนักงานใหญ่ เมื่อปี 2558 ที่มีผู้เสียชีวิตหลายรายเนื่องจากระบบดับเพลิงอัตโนมัติที่ถูกติดตั้งอยู่ภายในห้องเก็บเอกสารเป็นระบบเซ็นเซอร์ป้องกันเพลิงไหม้แบบอัตโนมัติ ที่ใช้แก๊สไพโรเจนซึ่งไล่ออกซิเจนในบริเวณที่เกิดเพลิงไหม้ออกไป ส่งผลให้บุคคลที่เข้าไประงับเหตุขาดอากาศหายใจและเสียชีวิตในที่สุด ดังนั้นการใช้อุปกรณ์หรือเทคโนโลยีทั้งหลายต้องมีคนคุมและมีการแจ้งเตือนแก่ผู้ที่เกี่ยวข้อง

2) องค์ประกอบเกี่ยวกับแผนปฏิบัติในสภาวะปกติและสภาวะฉุกเฉิน เช่น ในกรณีที่องค์การตั้งอยู่ในพื้นที่ที่เป็นจุดยุทธศาสตร์ เช่น มหาวิทยาลัยเทคโนโลยีราชมงคลพระนครมีพื้นที่อยู่ติดกับทำเนียบรัฐบาล ความเสี่ยงที่อาจเกิดขึ้นประการหนึ่งคือการชุมนุมประท้วง (ม็อบ) ซึ่งเมื่อเกิดเหตุการณ์ในลักษณะนี้ขึ้นให้ถือว่าองค์การอยู่ในสภาวะที่ไม่ปกติหรือสภาวะฉุกเฉิน ดังนั้นองค์การจึงต้องมีแผนรับมือหรือปฏิบัติการในสภาวะฉุกเฉินด้วย

3) องค์ประกอบเกี่ยวกับการวิเคราะห์และประเมินสภาพแวดล้อม หรือการกำหนดระดับความสำคัญของพื้นที่ (Casing) โดยผู้ที่ทำงานที่เกี่ยวข้องกับงานรักษาความปลอดภัยต้องศึกษาสภาพแวดล้อมโดยรอบขององค์การและวิเคราะห์สิ่งบอกเหตุเพื่อสามารถกำหนดมาตรการและแนวปฏิบัติเพื่อจัดการกับสถานการณ์ที่อาจเกิดขึ้นได้

4) องค์ประกอบเกี่ยวกับการสร้างเครือข่ายระหว่างหน่วยงาน ผู้เข้าร่วมสนทนากลุ่มส่วนใหญ่มองว่าภาคเอกชนขาดเรื่องของการสร้างเครือข่ายระหว่างองค์การที่ช่วยให้เกิดการแลกเปลี่ยนและติดตามความเคลื่อนไหวของปัจจัยที่อาจส่งผลกระทบต้องความมั่นคงปลอดภัยขององค์การได้

5) องค์ประกอบเกี่ยวกับนโยบายเกี่ยวกับงานด้านการรักษาความปลอดภัย ต้องสอดคล้องกับการนำไปปฏิบัติให้เกิดเป็นรูปธรรม ซึ่งในความเป็นจริงสวนทางกัน เนื่องจากว่างานด้านการรักษาความปลอดภัยเป็นเรื่องที่ทำให้เกิดความไม่สะดวกสบาย ดังนั้นอาจมีการลดระดับความเข้มข้นของมาตรการลงตามความรู้สึกหรือความต้องการของบุคคลที่ทำงานในองค์การนั้น ซึ่งไม่ถูกต้องและไม่ได้สะท้อนให้เห็นถึงความใส่ใจต้องมาตรการการรักษาความปลอดภัยอย่างแท้จริง

6) องค์ประกอบเกี่ยวกับกายภาพของมนุษย์ พิจารณาจากสรีระของผู้ที่ทำหน้าที่รักษาความปลอดภัยที่ควรมีรูปร่างสูงใหญ่ กำยำเป็นที่น่าเกรงขามแก่บุคคลที่จะก่อเหตุ

7) องค์ประกอบเกี่ยวกับการฝึกปฏิบัติมาตรการรักษาความปลอดภัยอย่างสม่ำเสมอ

ทั้ง 7 องค์ประกอบนี้เป็นองค์ประกอบที่ผู้เข้าร่วมการสนทนากลุ่มได้นำเสนอและพิจารณาว่ามีความสำคัญต้องระบบการรักษาความปลอดภัยขององค์การและควรถูกนำไปใช้ในการประเมินองค์ประกอบของระบบการรักษาความปลอดภัยสำหรับหน่วยงานเอกชนด้วย

5.3 ข้อเสนอแนะ

ผู้บริหารองค์การภาคเอกชนสามารถนำผลการศึกษาในครั้งนี้ที่ได้จากการวิเคราะห์เอกสารและผลการสนทนากลุ่มจากบุคคลที่เกี่ยวข้องกับการปฏิบัติงานด้านการรักษาความปลอดภัยทั้งจากหน่วยงานภาครัฐและเอกชน นำไปสู่การกำหนดเกณฑ์การประเมินมาตรการการรักษาความปลอดภัย ได้แก่ การสร้างความตระหนักรู้เกี่ยวกับการพัฒนาด้านเทคโนโลยีที่เกี่ยวข้องกับการรักษาความปลอดภัย การบูรณาการองค์ประกอบด้านสถาปัตยกรรม การพัฒนาระบบการรักษาความปลอดภัย การจัดการทรัพยากรมนุษย์ที่ครอบคลุมเจ้าหน้าที่รักษาความปลอดภัยและการให้ความรู้ที่เกี่ยวข้องกับบุคลากรในองค์การ และการกำหนดหลักปฏิบัติด้านการรักษาความปลอดภัยที่สอดคล้องกับธรรมชาติและกายภาพขององค์การ และอาจมีการนำไปจัดทำแบบสอบถามพร้อมทั้งการวิเคราะห์องค์ประกอบเพื่อนำไปสู่การพัฒนาตัวชี้วัดเพื่อใช้ในการกำหนดเกณฑ์มาตรฐานที่เหมาะสมแก่องค์การต่อไป

นอกจากนี้การให้ผู้เชี่ยวชาญด้านการรักษาความปลอดภัยได้มีส่วนร่วมในการประเมิน องค์ประกอบเกี่ยวกับงานด้านรักษาความปลอดภัยขององค์การทั้งในส่วนของการใช้เทคนิคเดลฟายหรือการใช้การวิเคราะห์องค์ประกอบเชิงยืนยันจะยิ่งช่วยทำให้องค์ประกอบที่ถูกสังเคราะห์และวิเคราะห์ออกมามีความน่าเชื่อถือมากยิ่งขึ้น และสามารถนำไปปรับใช้ในการกำหนดแผนการบริหารงานด้านการรักษาความปลอดภัยขององค์การและรายบุคคลภายในองค์การได้อย่างมีประสิทธิภาพมากยิ่งขึ้น

บรรณานุกรม

กรมพินิจและคุ้มครองเด็กและเยาวชน. (2551). **การรักษาความปลอดภัยเกี่ยวกับสถานที่.** [ออนไลน์] แหล่งที่มา : http://www2.djop.moj.go.th/knowledge/safty%20ubon%20cent.pdf

เดชน์ จรูญเรืองฤทธิ์. (2549). **ความรู้พื้นฐานเรื่องการรักษาความปลอดภัยสำหรับผู้บริหาร**. กรุงเทพมหานคร : สำนักพิมพ์แห่งจุฬาลงกรณ์มหาวิทยาลัย.

ดำรง ขำเปลี่ยน. (2543). **จิตสำนึกของผู้ขับขี่รถจักรยานยนตร์รับจ้างต่อความปลอดภัยในชีวิตและทรัพย์สิน.** วิทยานิพนธ์ สส.ม. (สาขาการบริหารและนโยบายสวัสดิการสังคม) คณะสังคมสงเคราะห์ศาสตร์ มหาวิทยาลัยธรรมศาสตร์.

นฤมล มณีงาม (2547). **การพัฒนาโปรแกรมสร้างจิตสำนึกเกี่ยวกับการประหยัดพลังงานตามหลักการเรียนรู้ด้วยการรับใช้สังคม สำหรับนักเรียนชั้นประถมศึกษาปีที่ 6.** วิทยานิพนธ์ ค.ม. (ประถมศึกษา) กรุงเทพมหานคร : บัณฑิตวิทยาลัย จุฬาลงกรณ์มหาวิทยาลัย.

ภาสกร สถิตยุทธการ. (2545). **การรักษาความปลอดภัยบุคคลสำคัญ: ศึกษาเฉพาะกรณีกองกำกับการอารักขาและรักษาความปลอดภัยบุคคลสำคัญ กองบังคับการสายตรวจและปฏิบัติการพิเศษ.** สารนิพนธ์ ศศ.ม. (การบริหารงานยุติธรรม) คณะสังคมสงเคราะห์ศาสตร์ มหาวิทยาลัยธรรมศาสตร์.

สนิท ปิ่นประดับ. (2548). **จิตสำนึกในการปฏิบัติงานเพื่อความปลอดภัยในการทำงานของช่างไฟฟ้า: ศึกษากรณีมหาวิทยาลัยเกษตรศาสตร์ วิทยาเขตบางเขน.** วิทยานิพนธ์ ค.ม. (เทคโนโลยีอุตสาหกรรม) บัณฑิตวิทยาลัย: มหาวิทยาลัยราชภัฏพระนคร.

สำนักข่าวกรองแห่งชาติ. (2551). **ระเบียบว่าด้วยการรักษาความปลอดภัยแห่งชาติ พ.ศ. 2517.** [ออนไลน์] แหล่งที่มา : http://www.nia.go.th/nia/content/showsubdetail.asp?fdcode=2115112162111211&dsc=+%C3%D0%E0%BA%D5%C2%BA%C7%E8%D2%B4%E9%C7%C2%A1%D2%C3%C3%D1%A1%C9%D2%A4%C7%D2%C1%BB%C5%CD%B4%C0%D1%C2%E1%CB%E8%A7%AA%D2%B5%D4+%BE%2E%C8%2E+2517

สำนักข่าวกรองแห่งชาติ. (2553). **ระเบียบสำนักนายกรัฐมนตรีว่าด้วยการรักษาความปลอดภัยแห่งชาติ พ.ศ. 2552** [ออนไลน์] แหล่งที่มา : http://www.nia.go.th/nia/content/showsubdetail.asp?fdcode=3215112162211211&dsc=+%C3%D0%E0%BA%D5%C2%BA%CA%D3%B9%D1%A1%B9%D2%C2%A1%C3%D1%B0%C1%B9%B5%C3%D5%C7%E8%D2%B4%E9%C7%C2%A1%D2%C3%C3%D1%A1%C9%D2%A4%C7%D2%C1%BB%C5%CD%B4%C0%D1%C2%E1%CB%E8%A7%AA%D2%B5%D4+%BE%2E%C8%2E2552

ศิโรรัตน์ ปิ่นประดับ. (2548). **จิตสำนึกการให้บริการของพนักงานธนาคารกรุงเทพจำกัด (มหาชน): ศึกษาเฉพาะกรณี สำนักธุรกิจ สยามสแควร์.** วิทยานิพนธ์ รป.ม. (การบริการทั่วไป) มหาวิยาลัยบูรพา.

อัจฉรา โฉมแฉล้ม. (2544). **จิตสำนึกของนักศึกษามหาวิทยาลัยธรรมศาสตร์ต่อการร่วมกลุ่มกิจกรรมเพื่อสังคม.** วิทยานิพนธ์ สส.ม. (สาขาการบริหารและนโยบายสวัสดิการสังคม) คณะสังคมสงเคราะห์ศาสตร์ มหาวิทยาลัยธรรมศาสตร์.

Burns, R. (1990). **Introduction to research methods.** Melbourne: Longman Chesire.

Cisco. (2007). **Cisco security awareness: Creating an effective security culture through awareness.** Retrieved from http://www.cisco.com/web/about/security/cspo/docs/SecurityAwarenessProgram.pdf

Demkin, J. A. (2003). **Security planning and design: a guide for architects and buiding design professionals.** New Jersey : John Wiley & Sons, Inc.

Fay, J. J. (2006). **Contemporary security management. (2nd ed.).** MA: Elsevier Butterworth-Heinemann.

Ficher, R. J., Halibozek, E., & Green, G. (2008). **Introduction to security. (8th ed.).** MA: Elsevier Butterworth-Heinemann.

Hutter, D. (2016). *Physical security and why it is important.* Retrieved from https://www.sans.org/reading-room/whitepapers/physical/physical-security-important-37120

Kurtus, R. (2001). **Theory of security.** [Online] Available : http://www.school-for-champions.com/security/theory.htm

LeBlanc, B. (n.d.). *Physical security.* Retrieved from http://faculty.uml.edu/bleblanc/44.115/pdf/Physical%20Security.pdf

Mills, A. (2001). "A systematic approach to risk management for construction" **Structural Survey** 19(5): 245-252.

Ortmeier, P.J. (2005). **Introduction to security :operations and management. (3rd ed.).** NJ: Prentice Hall.

Pallant, J. (2001). **SPSS survival manual: A step-by-step guide to data analysis.** Buckingham: Open University Press.

Patterson, D. G. (2004). Adapting security operating procedures to threat levels. *Journal of Facilities Management, 3*(1), 53-64.

Roper, C. A., Grau, J. A., & Fischer, L. F. (2005). **Security education awareness, and training: from theory to practice.** MA: Elsevier Butterworth-Heinemann.

Sennewald, C. A. (2003). **Effective security management (3rd ed.).** MA: Elsevier Butterworth-Heinemann.

Wiersma, W. (1991). **Research methods in education. (5th ed.).** Sydney: Allyn and Bacon.

Wulgaert, T. (2005). **Security awareness: Best practices to serve your enterprise**. IL: Information System Audit and Control Association.