ธรรมาภิบาลข้อมูลด้านความมั่นคง

กองอำนวยการรักษาความมั่นคงภายในราชอาณาจักร

พ.ศ. ๒๕๖๕

คำนำ

กอ.รมน. ได้ตระหนักถึงความสำคัญของข้อมูลและการนำข้อมูลที่มีความเหมาะสม หลากหลาย ครบถ้วน และทันสมัย มาใช้สนับสนุนการดำเนินงานให้มีประสิทธิภาพ ถูกต้อง แม่นยำ ภายใต้กรอบหน้าที่และอำนาจตามที่ได้รับมอบหมาย ทั้งในด้านการบูรณาการ อำนวยการ ประสานการปฏิบัติในการรักษาความมั่นคงภายในราชอาณาจักร ที่สอดคล้องกับยุทธศาสตร์ชาติ นโยบายของรัฐบาล หน่วยงานของรัฐ และความต้องการของประชาชน โดยมีเป้าหมายสูงสุดเพื่อให้ “ประเทศชาติมั่นคง ประชาชนมีความสุข”

อย่างไรก็ตาม การที่จะให้ได้มาซึ่งข้อมูลที่มีคุณสมบัติครบถ้วนดังที่กล่าวในข้างต้น กอ.รมน. จำเป็นต้องกำหนดนโยบายและแนวปฏิบัติเพื่อการบริหารจัดการในทุกขั้นตอนของวงจรชีวิตข้อมูล ตั้งแต่ การสร้างและจัดเก็บ การบูรณาการ การใช้ การเผยแพร่ การจัดเก็บถาวร และการทำลาย ทั้งที่เป็นข้อมูลที่อยู่ในกรอบความรับผิดชอบของหน่วยเอง และข้อมูลที่ กอ.รมน. บูรณาการการเชื่อมโยงมาจากแหล่งข้อมูลของหน่วยงานของรัฐและภาคเอกชน ในฐานะเป็นศูนย์กลางข้อมูลด้านความมั่นคงของประเทศ เพื่อนำไปวิเคราะห์ ประมวลผล และจัดทำให้อยู่ในรูปแบบรายงาน ภายใต้มาตรการรักษาความปลอดภัยและการรักษาความเป็นส่วนบุคคลของข้อมูล ก่อนนำเสนอให้รัฐบาล หน่วยงานความมั่นคง หรือผู้ที่มีหน้าที่เกี่ยวข้อง นำไปใช้ประโยชน์ได้โดยง่ายและมีประสิทธิภาพ

ดังนั้น เพื่อให้เกิดการบริหารจัดการข้อมูลที่มีประสิทธิภาพ กอ.รมน. จึงจัดทำธรรมาภิบาลข้อมูลด้านความมั่นคง กอ.รมน. พ.ศ. ๒๕๖๕ ฉบับนี้ขึ้น โดยได้ศึกษาสภาวะแวดล้อมทางด้านกฎหมาย นโยบาย บทบาท หน้าที่ และอำนาจ รวมทั้งกรอบแนวธรรมาภิบาลข้อมูลภาครัฐ หลักการ และมาตรฐานที่เกี่ยวข้อง มาใช้ประกอบการดำเนินการ เพื่อให้บุคลากรและส่วนงานต่าง ๆ ของ กอ.รมน. หน่วยงานของรัฐที่เกี่ยวข้องอื่น ๆ รวมทั้งผู้ที่มีส่วนได้ส่วนเสีย นำไปใช้ยึดถือปฏิบัติให้เป็นไปในทิศทางเดียวกัน อย่างเป็นระบบ ปลอดภัย โปร่งใส และเชื่อถือได้ ต่อไป

พลเอก

(ณรงค์พันธ์ จิตต์แก้วแท้)

รอง ผอ.รมน./ผู้บริหารระดับสูงสุด กอ.รมน.

สารบัญ

หน้า

บทที่ ๑
บทนำ

๑.๑ ความเป็นมา

ปัจจุบัน เป็นที่ยอมรับกันว่าการขับเคลื่อนองค์กร ไม่ว่าจะเป็นหน่วยงานที่มีขนาดเล็กหรือขนาดใหญ่ ทั้งภาครัฐและเอกชน ต่างมิอาจหลีกเลี่ยงการนำข้อมูลที่เกี่ยวข้อง มาบูรณาการและนำไปใช้สนับสนุนการบริหารจัดการเพื่อให้บรรลุผลสัมฤทธิ์ตามวัตถุประสงค์และเป้าหมายขององค์กร

ในการจัดทำกรอบแผนแม่บทภายใต้ยุทธศาสตร์ชาติประเด็นความมั่นคง ก็ได้เล็งเห็นถึงความสำคัญในการกำหนดทิศทางการดำเนินการดังกล่าว จึงได้กำหนดให้มีแผนบูรณาการข้อมูลระหว่างหน่วยงานด้านความมั่นคง ภายใต้แผนย่อยการบริหารจัดการความมั่นคงแบบองค์รวมขึ้น ซึ่งต่อมา สำนักงานสภาความมั่นคงแห่งชาติ (สมช.) ในฐานะหน่วยงานหลักที่รับผิดชอบแผนย่อยดังกล่าว ได้จัดทำรายละเอียด (ร่าง) แผนบูรณาการข้อมูลด้านความมั่นคงขึ้น และนำเรียนนายกรัฐมนตรี เพื่อกรุณาอนุมัติและให้ประกาศใช้ ตั้งแต่ ๒๗ ธันวาคม พ.ศ. ๒๕๖๒ โดยเปลี่ยนชื่อเป็น “แผนปฏิบัติการด้านการบูรณาการข้อมูลด้านความมั่นคง ระยะที่ ๑ พ.ศ. ๒๕๖๓ - ๒๕๖๕” และแบ่งมอบหน้าที่ให้กับหน่วยราชการที่เกี่ยวข้อง เป็น ๓ ระดับ ได้แก่ ระดับนโยบาย มี สมช. เป็นหน่วยรับผิดชอบ ระดับอำนวยการและประสานการปฏิบัติ ให้ กอ.รมน. เป็นหน่วยรับผิดชอบ รวมทั้งให้ทำหน้าที่เป็นศูนย์กลางข้อมูลด้านความมั่นคง (Data Center) ของประเทศ โดยมี ศรชล. และหน่วยงานของรัฐ ระดับ กระทรวง/กรม ที่เกี่ยวข้อง ทำหน้าที่เป็นหน่วยในระดับปฏิบัติในการพัฒนาข้อมูลที่อยู่ในความรับผิดชอบ รวมทั้งสนับสนุนการเชื่อมโยงแลกเปลี่ยนข้อมูลกับ กอ.รมน.

ทั้งนี้ การมอบภารกิจศูนย์กลางข้อมูลด้านความมั่นคงให้กับ กอ.รมน. ซึ่งเป็นหน่วยงานจัดตั้งขึ้นภายใต้พระราชบัญญัติการรักษาความมั่นคงภายในราชอาณาจักร พ.ศ. ๒๕๕๑ นั้น มีความมุ่งหมายเพื่อให้มีหน่วยงานกลางรับผิดชอบการรวบรวมข้อมูลด้านความมั่นคงและข้อมูลอื่น ๆ ที่เกี่ยวข้อง ซึ่งปัจจุบันได้ถูกจัดเก็บและใช้งานเป็นการภายในของแต่ละหน่วยงานเป็นการเฉพาะ ในลักษณะการนำเข้าข้อมูลมาจัดเก็บเป็นฐานข้อมูลขนาดใหญ่ที่จุด ๆ เดียว ผ่านการเชื่อมโยงแลกเปลี่ยนโดยใช้เทคโนโลยีที่เหมาะสมอย่างเป็นระบบ และหน่วยงานของรัฐอื่น ๆ ที่เกี่ยวข้อง ซึ่งมีฐานะเป็นหน่วยใช้ประโยชน์ สามารถเข้ามาใช้งานระบบบูรณาการข้อมูลเชิงวิเคราะห์ในรูปแบบรายงานอัจฉริยะ (Business Intelligences) ผ่านเครื่องมือที่ใช้สถาปัตยกรรมเทคโนโลยีสารสนเทศขั้นสูง เช่น ระบบการเรียนรู้โดยเครื่องจักร (Machine Learning : ML) ระบบการคิดแบบปัญญาประดิษฐ์ (Artificial Intelligence : AI) และระบบประมวลผลข้อมูลขนาดใหญ่ หรือบิ๊กดาต้าแพลตฟอร์ม (Big Data Platform) เพื่อเสนอให้ผู้บังคับบัญชา ผู้บริหาร ฝ่ายอำนวยการ หรือเจ้าหน้าที่ระดับปฏิบัติการ สามารถมองเห็นภาพ รับรู้ตระหนักรู้ เข้าถึงเหตุการณ์ หรือความเป็นไปของสถานการณ์ นำไปสู่การตัดสินใจ สั่งการ หรือปฏิบัติการได้อย่างถูกต้อง แม่นยำ และมีประสิทธิภาพ ซึ่งนับว่าเป็นเครื่องมือที่มีความสำคัญต่อการขับเคลื่อนการพัฒนากลไกการบริหารจัดการความมั่นคงแบบองค์รวมของประเทศ เป็นอย่างยิ่ง

อย่างไรก็ตาม ข้อมูลที่จะบูรณาการเข้ามาดำเนินการและใช้งานตามกรอบหน้าที่ที่ได้รับมอบหมายของศูนย์กลางข้อมูลด้านความมั่นคงนั้น เป็นสินทรัพย์ที่มีค่า (Data as an Asset) ที่มีความจำเป็นต้องบริหารจัดการและกำกับดูแลอย่างเป็นระบบ ด้วยความระมัดระวัง โดยกำหนดเป็นกรอบการธรรมาภิบาลข้อมูล เพื่อให้บุคลากรของหน่วยงานของรัฐที่เกี่ยวข้อง ซึ่งรวมถึงผู้ที่มีส่วนได้ส่วนเสีย ได้รับทราบและปฏิบัติตามนโยบายและแนวปฏิบัติได้อย่างมีประสิทธิภาพ ถูกต้อง และปลอดภัย ในทุกขั้นตอนบนวงจรชีวิตข้อมูล (Data Life Cycle) เช่น ขั้นตอนสร้างและจัดเก็บ (Create and Store) บูรณาการ (Integrate) ใช้ (Use) เผยแพร่ (Publish) จัดเก็บถาวร (Archive) และทำลาย (Destroy)

ทั้งนี้ ธรรมาภิบาลข้อมูลด้านความมั่นคง กอ.รมน. พ.ศ. ๒๕๖๕ ฉบับนี้ ได้นำนโยบาย หลักการ หลักแนวคิด รวมทั้ง กรอบธรรมาภิบาลข้อมูลภาครัฐ และมาตรฐานที่เป็นสากลอื่น ๆ มาใช้ประกอบการพิจารณาในการจัดทำขึ้น เพื่อให้บุคลากรของหน่วยงานของรัฐที่เกี่ยวข้อง และผู้ที่มีส่วนได้ส่วนเสีย ได้นำไปใช้ยึดถือปฏิบัติควบคู่กับระเบียบปฏิบัติและกฎหมายที่เกี่ยวข้อง ได้แก่ พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ พระราชบัญญัติข่าวกรองแห่งชาติ พ.ศ. ๒๕๖๒ และพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ ฯลฯ อย่างเป็นระบบต่อไป

๑.๒ วัตถุประสงค์การจัดทำ

ธรรมาภิบาลข้อมูลด้านความมั่นคง กอ.รมน. พ.ศ. ๒๕๖๕ ได้จัดทำขึ้นโดยมีวัตถุประสงค์ดังนี้

๑.๒.๑ เพื่อให้มีกรอบนโยบายและแนวปฏิบัติ ในการบริหารจัดการและกำกับดูแลข้อมูลด้านความมั่นคงภายใต้กรอบหน้าที่และอำนาจของ กอ.รมน. และบทบาทการเป็นศูนย์กลางข้อมูลด้านความมั่นคงของประเทศที่เป็นมาตรฐานสากล สอดคล้องกับหลักธรรมาภิบาลข้อมูลภาครัฐ รวมถึง ระเบียบ กฎหมาย และนโยบายภาครัฐอื่น ๆ ที่เกี่ยวข้อง

๑.๒.๒ เพื่อให้ผู้ที่มีส่วนได้ส่วนเสียเกี่ยวข้องกับข้อมูลด้านความมั่นคง ซึ่งเป็นเป้าหมายการบูรณาการและอยู่ในกรอบอำนาจหน้าที่ของศูนย์กลางข้อมูลด้านความมั่นคง ได้แก่ ผู้บังคับบัญชา ผู้บริหาร ฝ่ายอำนวยการหรือเจ้าหน้าที่ระดับปฏิบัติการของหน่วยงานของรัฐต่าง ๆ ใช้ยึดถือปฏิบัติและตรวจสอบการปฏิบัติ ร่วมกันอย่างเป็นระบบ

๑.๒.๓ เพื่อสร้างความเชื่อมั่นและอำนวยความสะดวกให้กับหน่วยงานของรัฐและภาคเอกชนที่สนับสนุนข้อมูลและการเชื่อมโยงแลกเปลี่ยนข้อมูล รวมทั้งการใช้ประโยชน์จากระบบบูรณาการข้อมูลเชิงวิเคราะห์ของศูนย์กลางข้อมูลด้านความมั่นคง

๑.๒.๔ เพื่อส่งเสริมการปรับปรุงพัฒนาระบบฐานข้อมูลของหน่วยงานของรัฐและภาคเอกชนที่เกี่ยวข้อง ให้เป็นมาตรฐานและเกื้อกูลต่อการเชื่อมโยงแลกเปลี่ยนข้อมูลกับศูนย์กลางข้อมูลด้านความมั่นคง

๑.๓ ขอบเขตเนื้อหาและแนวทางการใช้

ธรรมาภิบาลข้อมูลด้านความมั่นคง กอ.รมน. ได้แบ่งขอบเขตเนื้อหาออกเป็น ๖ บท เพื่อให้ผู้ที่มีส่วนได้ส่วนเสีย ใช้อ้างอิงหรือยึดถือปฏิบัติ โดยมีสาระสำคัญสรุปได้ดังนี้

๑.๓.๑ ในบทที่ ๑ เป็นการกล่าวนำโดยอธิบายถึงความเป็นมา วัตถุประสงค์ ขอบเขตและแนวทางการใช้งานเอกสารธรรมาภิบาลข้อมูลด้านความมั่นคง กอ.รมน. ฉบับนี้ โดยในช่วงท้ายของบท ได้นำเสนอข้อมูล

เกี่ยวกับนิยามศัพท์ที่ใช้ภายในเอกสาร ซึ่งจะช่วยให้ผู้ที่มีความเกี่ยวข้อง สนใจ ได้เข้าใจในความหมาย รวมทั้งป้องกันความเข้าใจที่คลาดเคลื่อนอีกด้วย

๑.๓.๒ ในบทที่ ๒ เป็นการนำเสนอข้อมูลที่ได้จากการศึกษาสภาพแวดล้อมที่มีอิทธิพลต่อการจัดทำธรรมาภิบาลข้อมูลด้านความมั่นคง กอ.รมน. โดยเริ่มจากเหตุผลความจำเป็นและกรอบแนวคิดในการขับเคลื่อนให้เกิดการบูรณาการข้อมูลในมิติความมั่นคงของประเทศ ซึ่งได้ส่งมอบภารกิจให้กับ กอ.รมน. เป็นหน่วยงานกลางทำหน้าที่เป็นศูนย์กลางข้อมูล และเป็นหน่วยระดับอำนวยการเพื่อประสานการปฏิบัติให้เกิดการเชื่อมโยงแลกเปลี่ยนข้อมูลระหว่างหน่วยงานของรัฐและภาคเอกชน ดังนั้น กอ.รมน. จึงจำเป็นต้องกำหนดแนวทางการบริหารจัดการข้อมูลหรืออีกนัยหนึ่งคือการธรรมาภิบาลข้อมูลให้เป็นระบบ ควบคู่กับการธรรมาภิบาลข้อมูลในความรับผิดชอบของหน่วยเอง และที่สำคัญในบทนี้ ได้สรุปกฎหมายและระเบียบที่เกี่ยวข้องทั้งหมด ทั้งในมิติด้านการธรรมาภิบาลข้อมูล การเปิดเผยข้อมูล การรักษาความลับและความปลอดภัย การรักษาความมั่นคงปลอดภัยไซเบอร์ และการคุ้มครองข้อมูลส่วนบุคคล ฯลฯ ทั้งนี้ เพื่อให้ผู้ที่สนใจ ได้ศึกษาและอ้างอิงประกอบการดำเนินงาน

๑.๓.๓ ในบทที่ ๓ เป็นการชี้แจงหลักการในการธรรมาภิบาลข้อมูล เริ่มจากการกำหนดวงจรชีวิตข้อมูลที่อยู่ในบริบทความรับผิดชอบของ กอ.รมน. ซึ่งแบ่งเป็น ๒ กลุ่ม หลายขั้นตอน ได้แก่ ขั้นตอนสร้างและจัดเก็บ บูรณาการ ใช้ เผยแพร่ จัดเก็บถาวร และทำลาย รวมทั้ง ได้อธิบายองค์ประกอบการบริหารจัดการข้อมูลในแต่ละขั้นตอนวงจรชีวิตข้อมูล หลังจากนั้นเป็นการนำขอบเขตงานธรรมาภิบาลข้อมูลภาครัฐ ที่คณะกรรมการพัฒนารัฐบาลดิจิทัลได้ประกาศใช้ มาผนวกกับทฤษฎีวงจรเดมมิ่ง เพื่อกำหนดแนวทางขับเคลื่อนและพัฒนางานธรรมาภิบาลข้อมูล กอ.รมน. ให้เป็นระบบและชัดเจน

๑.๓.๔ ในบทที่ ๔ - บทที่ ๖ เป็นบทที่มีเนื้อหาสำคัญที่สุด เนื่องจากเป็นการกล่าวถึงแนวทางการนำธรรมาภิบาลข้อมูลไปสู่การปฏิบัติ ตั้งแต่การกำหนดทิศทาง วิสัยทัศน์ นโยบาย มาตรฐานและแนวปฏิบัติ รวมทั้ง โครงสร้างบุคลากรที่เกี่ยวข้องในภาพรวม โดยในบทที่ ๕ ได้สรุปโครงสร้างบุคลากร มาตรฐานและแนวปฏิบัติเกี่ยวกับการธรรมาภิบาลข้อมูลในระดับส่วนงานของ กอ.รมน. ซึ่งถือว่าเป็นเจ้าของข้อมูลและต้องควบคุมข้อมูลที่อยู่ในความรับผิดชอบข้อมูลที่หน่วยครอบครองหรือใช้งานอยู่ และท้ายสุด ในบทที่ ๖ เป็นการชี้แจงกรอบมาตรฐานและแนวปฏิบัติที่เกี่ยวกับการธรรมาภิบาลข้อมูลระดับบูรณาการ ซึ่งได้จากการเชื่อมโยงแลกเปลี่ยนเข้ามายังศูนย์กลางข้อมูลด้านความมั่นคง และนำไปวิเคราะห์ประมวลผล เพื่อการเผยแพร่หรือนำเสนอในรูปแบบรายงานอัจฉริยะให้หน่วยงานหรือผู้ที่เกี่ยวข้องนำไปใช้ประโยชน์ ตามลำดับ

๑.๓.๕ ในส่วนท้ายของเอกสารธรรมาภิบาลข้อมูลด้านความมั่นคง กอ.รมน. ได้จัดทำภาคผนวกเพื่อแนบรายละเอียดเพิ่มเติม แบ่งเป็น ๔ ส่วน ดังนี้

๑.๓.๕.๑ ผนวก ก เป็นข้อมูลบรรณานุกรม ซึ่งเป็นบัญชีอ้างอิงแหล่งที่มาของข้อมูลที่ใช้ภายในเอกสารธรรมาภิบาลข้อมูลด้านความมั่นคง กอ.รมน.

๑.๓.๕.๒ ผนวก ข เป็นบัญชีรายการ ระเบียบ แนวทาง ข้อปฏิบัติ ข้อกำหนด หรือมาตรฐานในการดำเนินการธรรมาภิบาลข้อมูลตามนโยบาย มาตรฐานและแนวปฏิบัติที่กำหนด

๑.๓.๕.๓ ผนวก ค เป็นบัญชีรายการ แบบฟอร์มที่ใช้สำหรับการบันทึก จัดเก็บประวัติ หรือผลการดำเนินการธรรมาภิบาลข้อมูลตามนโยบาย มาตรฐานและแนวปฏิบัติที่กำหนด

๑.๓.๕.๔ ผนวก ง เป็นบัญชีรายการ ตัวอย่างเอกสารหรือคำแนะนำในการดำเนินการธรรมาภิบาลข้อมูลตามนโยบาย มาตรฐานและแนวปฏิบัติที่กำหนด

๑.๓.๖ มอบหมายให้ผู้อำนวยการศูนย์ดิจิทัลเพื่อความมั่นคง กอ.รมน. ในฐานะหัวหน้าทีมบริกรข้อมูล กอ.รมน. เป็นผู้รักษาการตามธรรมาภิบาลข้อมูลด้านความมั่นคง กอ.รมน. ฉบับนี้ ทั้งนี้ หากมีความจำเป็น ให้พิจารณาปรับปรุงเนื้อหาในทันที หรือทบทวนรายละเอียดให้มีความเหมาะสมทันสมัย อย่างเป็นวงรอบ อย่างน้อยปีงบประมาณละ ๑ ครั้ง

๑.๔ นิยามศัพท์ทั่วไปที่สำคัญ

ธรรมาภิบาลข้อมูลด้านความมั่นคง กอ.รมน. ฉบับนี้ ได้จัดทำนิยามศัพท์ที่สำคัญ แบ่งเป็น ๒ ส่วน ส่วนแรกนำเสนอในบทที่ ๑ ข้อ ๑.๔ เป็นการกำหนดนิยามศัพท์ทั่วไปที่ใช้ในเอกสารฉบับนี้ และส่วนที่ ๒ นำเสนอในบทที่ ๔ เป็นการนิยามศัพท์ด้านธรรมาภิบาลข้อมูล ซึ่งจำเป็นต้องกำหนดให้มีความชัดเจนตามกรอบธรรมาภิบาลข้อมูลภาครัฐ สำหรับนิยามศัพท์ทั่วไป สรุปได้ดังนี้

๑.๔.๑ “ความมั่นคง” หมายถึง ภาวะที่ประเทศชาติปลอดจากภัยคุกคามต่อเอกราช มีอธิปไตย บูรณภาพแห่งอาณาเขต สถาบันศาสนา สถาบันพระมหากษัตริย์ ความปลอดภัยของประชาชน การดำรงชีวิตโดยปกติสุขของประชาชน หรือที่กระทบต่อผลประโยชน์แห่งชาติหรือการปกครองระบอบประชาธิปไตยอันมีพระมหากษัตริย์ทรงเป็นประมุข รวมทั้งความพร้อมของประเทศที่จะเผชิญสถานการณ์ต่าง ๆ อันเกิดจากภัยคุกคามทุกรูปแบบ

๑.๔.๒ “ข้อมูล (Data)” หมายถึง สิ่งที่สื่อความหมายให้รู้เรื่องราวข้อเท็จจริงหรือเรื่องอื่นใดไม่ว่าการสื่อความหมายนั้นจะทำได้โดยสภาพของสิ่งนั้นเองหรือโดยผ่านวิธีการใด ๆ และไม่ว่าจะได้จัดทำไว้ในรูปของเอกสาร แฟ้มรายงาน หนังสือ แผนผัง แผนที่ ภาพวาด ภาพถ่าย ภาพถ่ายดาวเทียม ฟิล์มการบันทึกภาพหรือเสียง การบันทึกโดยเครื่องคอมพิวเตอร์ เครื่องมือตรวจวัดการสำรวจระยะไกลหรือวิธีอื่นใดที่ทำให้สิ่งที่บันทึกไว้ปรากฏ

๑.๔.๓ “ข้อมูลด้านความมั่นคง” หมายถึง ข้อมูลที่มีความเกี่ยวข้องความมั่นคงของรัฐ เอกราช อธิปไตย บูรณภาพแห่งอาณาเขต สถาบันศาสนา สถาบันพระมหากษัตริย์ ความปลอดภัยของประชาชน การดำรงชีวิตโดยปกติสุขของประชาชน หรือที่กระทบต่อผลประโยชน์แห่งชาติหรือการปกครองระบอบประชาธิปไตยอันมีพระมหากษัตริย์ทรงเป็นประมุข รวมทั้งความพร้อมของประเทศที่จะเผชิญสถานการณ์ต่าง ๆ อันเกิดจากภัยคุกคามทุกรูปแบบ

๑.๔.๔ “ศูนย์กลางข้อมูลด้านความมั่นคง” หมายถึง บทบาทของ กอ.รมน. ที่ทำหน้าที่เป็นจุดศูนย์รวมข้อมูลด้านความมั่นคง โดยเชื่อมโยงแลกเปลี่ยนกับหน่วยงานของรัฐและภาคเอกชน และนำเข้ามาจัดหมวดหมู่และจัดเก็บอย่างเป็นระบบให้เป็นข้อมูลขนาดใหญ่ในคลังข้อมูลหรือดาตาเลค ฯลฯ เพื่อทำการวิเคราะห์ประมวลผล และนำเสนอในรูปแบบรายงานอัจฉริยะ สนับสนุนให้หน่วยงาน และบุคลากรที่เกี่ยวข้องใช้งานด้วยอุปกรณ์และระบบเทคโนโลยีสารสนเทศขั้นสูง ได้แก่ ระบบปัญญาประดิษฐ์ ระบบการเรียนรู้ของเครื่องและบิ๊กดาต้าแพลตฟอร์ม ฯลฯ

๑.๔.๕ “การธรรมาภิบาลข้อมูล” หมายถึง การกำหนดสิทธิ หน้าที่ และความรับผิดชอบของผู้มีส่วนได้ส่วนเสียในการบริหารและจัดการข้อมูลทุกขั้นตอน เพื่อให้การได้ข้อมูล และการนำข้อมูลไปใช้มีความถูกต้อง

สมบูรณ์ เป็นปัจจุบัน และรักษาความเป็นส่วนบุคคลของข้อมูล รวมถึงสามารถแลกเปลี่ยนข้อมูลระหว่างหน่วยงานได้อย่างมีประสิทธิภาพ

๑.๔.๖ “วงจรชีวิตข้อมูล (Data Life Cycle)” หมายถึง กระบวนการจัดการข้อมูลซึ่งมีลักษณะเป็นวงรอบเปรียบเสมือนกับวงจรชีวิต ที่มีการเกิด แก่ เจ็บ และตาย โดยวงจรชีวิตข้อมูลทั่วไป เริ่มตั้งแต่การสร้าง การจัดเก็บ การใช้ การเผยแพร่ การจัดเก็บถาวร และการทำลายข้อมูล

๑.๔.๗ “การบริหารจัดการข้อมูล” หมายถึง กระบวนการจัดการเพื่อควบคุมข้อมูลให้สามารถนำไปใช้งานได้อย่างมีคุณภาพ โดยองค์ประกอบสำคัญที่เป็นเครื่องมือในการดำเนินการ รวม ๑๐ องค์ประกอบ ได้แก่ การบริหารจัดการสถาปัตยกรรมข้อมูล การสร้างแบบจำลองและออกแบบข้อมูล การจัดเก็บและการดำเนินงานต่อข้อมูล การบูรณาการและความสามารถในการทำงานร่วมกัน การบริหารจัดการเอกสารและเนื้อหา การบริหารจัดการข้อมูลหลักและข้อมูลอ้างอิง การบริหารจัดการคลังข้อมูล ดาตาเลค และระบบรายงานอัจฉริยะ การบริหารจัดการเมทาดาตา การบริหารจัดการความมั่นคงปลอดภัยและการรักษาความเป็นส่วนบุคคลของข้อมูล และการบริหารจัดการคุณภาพของข้อมูล

๑.๔.๘ “การบูรณาการข้อมูล” หมายถึง กระบวนการรวบรวม ประสาน จัดเก็บและเชื่อมโยงความสัมพันธ์ของข้อมูลที่มีเนื้อหา รูปแบบ หรือประเภทที่หลากหลาย จากระบบหรือแหล่งข้อมูลต่าง ๆ โดยมีเป้าหมายเพื่อการจัดทำมาตรฐานข้อมูลกลางสำหรับการแบ่งปันและเผยแพร่เพื่อการใช้ประโยชน์ร่วมกัน

๑.๔.๙ “การประมวลผลข้อมูล” หมายถึง การดำเนินการหรือชุดการดำเนินการใด ๆ ซึ่งกระทำต่อข้อมูลหรือชุดข้อมูล ไม่ว่าจะด้วยวิธีการอัตโนมัติหรือไม่ เช่น การเก็บ บันทึก จัดระบบ จัดโครงสร้าง เก็บรักษา เปลี่ยนแปลงหรือปรับเปลี่ยน การรับ พิจารณา ใช้ เปิดเผยด้วยการส่งต่อ เผยแพร่ หรือกระทำอื่นใดซึ่งทำให้เกิดความพร้อมใช้งาน การจัดวางหรือผสมเข้าด้วยกัน การจำกัด การลบ หรือการทำลาย

๑.๔.๑๐ “รูปแบบรายงานอัจฉริยะ (Business Intelligences)” [๑] หมายถึง การจัดทำรายงานในรูปแบบต่าง ๆ จากข้อมูลขนาดใหญ่และมีความซับซ้อน โดยใช้โปรแกรมประยุกต์ที่ใช้เทคโนโลยีขั้นประยุกต์เพื่อนำเสนอมุมมองในการวิเคราะห์ สังเคราะห์ แสดงความสัมพันธ์ และทำนายผลลัพธ์หรือแนวโน้มที่อาจเกิดขึ้นได้ตรงตามความต้องการของผู้ใช้งาน

๑.๔.๑๑ “การรักษาความปลอดภัยของข้อมูล” หมายถึง การรักษาความลับ ความถูกต้องของข้อมูล และความพร้อมใช้งานของข้อมูล โดยดำเนินการตั้งแต่การวางแผน การจัดทำ การปฏิบัติและบังคับใช้นโยบาย รวมถึงการดำเนินการอื่นใดเกี่ยวกับข้อมูล ทั้งนี้ ต้องคำนึงถึงการรักษาความเป็นส่วนบุคคลของข้อมูลเป็นสำคัญ

๑.๔.๑๒ “บิ๊กดาต้าแพลตฟอร์ม (Big Data Platform)” [๒] หมายถึงระบบข้อมูลขนาดใหญ่ ที่มีขีดความสามารถหลักรวม ๔ ด้าน ได้แก่ (๑) การรวบรวมและจัดการข้อมูลจากแหล่งข้อมูลต่าง ๆ ซึ่งมีจำนวนมากหลากหลาย เปลี่ยนแปลงอย่างรวดเร็ว มีคุณค่า แต่ยังเป็นข้อมูลปฐมภูมิหรือข้อมูลดิบที่ยังไม่ได้รับการประมวลผล (๒) การจัดหมวดหมู่และจัดเก็บข้อมูล (๓) การวิเคราะห์ประมวลผลข้อมูล และ (๔) การนำเสนอข้อมูลรายงาน (Data Visualization) หรือรูปแบบรายงานอัจฉริยะ

๑.๔.๑๓ “ปัญญาประดิษฐ์ (Artificial Intelligence)” [๒] หมายถึงความสามารถของระบบคอมพิวเตอร์ หรือเครื่องมืออิเล็กทรอนิกส์ ที่ทำงานผ่านคำสั่งหรือชุดคำสั่ง ในการแสดงปฏิกิริยา หรือการกระทำใด ๆ ในสถานการณ์อย่างหนึ่งอย่างใด ด้วยตนเอง เสมือนการทำงานของมนุษย์

๑.๔.๑๔ “การเรียนรู้ของเครื่อง (Machine Learning)” [๒] หมายถึง ระบบการเรียนรู้ของเครื่องจักร ส่วนใหญ่หมายถึงระบบคอมพิวเตอร์ ที่พัฒนากระบวนการเรียนรู้ข้อมูลและพัฒนาข้อมูล จากชุดข้อมูลตัวอย่าง โดยอาศัยวิธีการทางสถิติ ในลักษณะ “การรู้จำรูปแบบ” และสร้างเป็น “แบบจำลอง (Model)” เพื่อการตัดสินใจ ในการดำเนินการในสถานการณ์เฉพาะใด ๆ ได้ด้วยตนเอง โดยไม่ต้องเขียนคำสั่ง ชุดคำสั่ง หรือโปรแกรม

บทที่ ๒
สภาพแวดล้อมที่เกี่ยวกับธรรมาภิบาลข้อมูลของ กอ.รมน.

๒.๑ กล่าวนำ

ขอบเขตภาระงานการบูรณาการข้อมูลของ กอ.รมน. แบ่งออกได้เป็น ๒ ส่วน ประกอบด้วย การบูรณาการข้อมูลที่อยู่ในความรับผิดชอบตามกรอบอำนาจหน้าที่การรักษาความมั่นคงภายในราชอาณาจักร และการบูรณาการข้อมูลในฐานะศูนย์กลางข้อมูลด้านความมั่นคงของประเทศ ซึ่งต้องสถาปนาระบบเชื่อมโยงแลกเปลี่ยนและการวิเคราะห์ประมวลผลข้อมูล กับหน่วยงานของรัฐและองค์กรภาคเอกชน สนับสนุนแผนย่อยการพัฒนากลไกการบริหารจัดการความมั่นคงแบบองค์รวม แผนแม่บทภายใต้ยุทธศาสตร์ชาติประเด็นความมั่นคง พ.ศ. ๒๕๖๑ – ๒๕๘๐ ซึ่งนับว่าเป็นเรื่องที่มีความสำคัญและมีรายละเอียดจำนวนมาก ดังนั้น กอ.รมน. จึงจำเป็นต้องรวบรวมข้อมูลและศึกษาสภาพแวดล้อมที่เกี่ยวข้องกับการบูรณาการและบริหารจัดการข้อมูลทั้งในด้านนโยบาย ยุทธศาสตร์ ระเบียบ และกฎหมาย ฯลฯ เพื่อจัดทำธรรมาภิบาลข้อมูลด้านความมั่นคง กอ.รมน. อย่างเป็นระบบ โปร่งใส ชัดเจน และเชื่อถือได้

ในบทที่ ๒ นี้ เป็นการกล่าวสรุปสภาพแวดล้อมที่มีอิทธิพลต่อการบูรณาการข้อมูล ทั้งในด้านความสำคัญ หน้าที่ นโยบาย ภารกิจ ระเบียบ และกฎหมาย ฯลฯ เพื่อให้ผู้ที่มีความเกี่ยวข้อง มีความเข้าใจและรับทราบเหตุผลความจำเป็นวัตถุประสงค์ เป้าหมาย และขอบเขตการดำเนินงานในภาพรวม ก่อนลงรายละเอียดในบทอื่น ๆ ต่อไป

๒.๒ ความสำคัญของข้อมูลและการบูรณาการข้อมูล

รัฐบาลได้ให้ความสำคัญต่อการขับเคลื่อนการพัฒนาด้านดิจิทัลของหน่วยงานภาครัฐ ผ่านยุทธศาสตร์ชาติ ๒๐ ปี ด้านการปรับสมดุลและพัฒนาระบบการบริหารจัดการภาครัฐ แผนแม่บทภายใต้ยุทธศาสตร์ชาติประเด็นการบริการประชาชนและประสิทธิภาพภาครัฐ (พ.ศ. ๒๕๖๑ - ๒๕๘๐) แผนปฏิรูปประเทศด้านการปรับสมดุลภาครัฐและยุทธศาสตร์ภายใต้แผนพัฒนาเศรษฐกิจและสังคมแห่งชาติด้านการปรับเปลี่ยนภาครัฐสู่การเป็นรัฐบาลดิจิทัล โดยได้นำไปสู่การปฏิบัติภายใต้กรอบกฎหมายที่เกี่ยวข้อง ได้แก่ พระราชบัญญัติการพัฒนาดิจิทัลเพื่อเศรษฐกิจและสังคม พ.ศ. ๒๕๖๐ [๓] ซึ่งได้กำหนดวิสัยทัศน์ “ปฏิรูปประเทศไทยสู่ดิจิทัลไทยแลนด์ (Digital Thailand)” เพื่อให้สามารถสร้างสรรค์และใช้ประโยชน์จากเทคโนโลยีดิจิทัลอย่างเต็มศักยภาพในการพัฒนาโครงสร้างพื้นฐาน นวัตกรรม ข้อมูล ทุนมนุษย์ และทรัพยากรอื่นใด สนับสนุนการพัฒนาเศรษฐกิจและสังคมของประเทศไปสู่ความมั่นคง มั่งคั่ง และยั่งยืน นำไปสู่การจัดทำแผนพัฒนารัฐบาลดิจิทัลของประเทศ (พ.ศ. ๒๕๖๓ - ๒๕๖๕) [๔] ที่มีเป้าหมายหลักเพื่อการปรับปรุงประสิทธิภาพการทำงาน การเปิดเผยข้อมูล และการบริการประชาชน เช่น การจัดให้มีบริการอัจฉริยะ (Smart Service) ที่ขับเคลื่อนโดยความต้องการของประชาชน หรือผู้ใช้บริการ (Citizen Driven) การปรับเปลี่ยนการทำงานภาครัฐด้วยเทคโนโลยีดิจิทัลให้มีประสิทธิภาพและธรรมาภิบาล การสนับสนุนให้มีการเปิดเผยข้อมูลที่เป็นประโยชน์ (Open Data) และให้มีประชาชนมีส่วนร่วมในกระบวนการทำงานของภาครัฐ (Open Government) และการพัฒนาแพลตฟอร์มบริการพื้นฐานภาครัฐ (Government Service Platform) เป็นต้น

ผลิตผลจากการขับเคลื่อนงานพัฒนาด้านดิจิทัลของแต่ละหน่วยงานของรัฐที่กล่าวในข้างต้น ก่อให้เกิดข้อมูลจำนวนมาก ถึงแม้ข้อมูลมีแหล่งกำเนิดหรือรูปแบบโครงสร้างที่แตกต่างกัน แต่ด้วยเทคโนโลยีข้อมูลขนาดใหญ่ (Big Data Technology) ที่มีอยู่ในปัจจุบัน ทำให้สามารถบูรณาการให้เกิดการเชื่อมโยงข้อมูลเข้าด้วยกันในหลายแนวทาง เช่น แนวทางการดำเนินการบูรณาการฐานข้อมูลประชาชนและการบริการภาครัฐ โดยสำนักบริหารการทะเบียน กรมการปกครอง กระทรวงมหาดไทย เป็นหน่วยงานกลางในการเชื่อมโยงฐานข้อมูลประชาชนของส่วนราชการ (Population Information Linkage Center) และทำหน้าที่เป็นผู้ให้บริการข้อมูล (Gate Way) ตามที่หน่วยงานของรัฐร้องขอ เพื่อนำไปใช้งาน วิเคราะห์ประมวลผล และนำเสนอในรูปแบบที่เหมาะสมสนับสนุนงานบริการประชาชน รวมถึงกระบวนการตัดสินใจหรือการทำงานขององค์กรได้อย่างมีประสิทธิภาพ ฯลฯ อันเป็นการเกื้อกูลต่อหลักการเปลี่ยนผ่านไปสู่องค์กรที่ขับเคลื่อนด้วยข้อมูล (Data Driven Organization) [๕] ซึ่งแนวทางดังกล่าว จะเป็นพลังอำนาจที่สำคัญของทุกหน่วยงานในอนาคต ทั้งในระดับประเทศ หน่วยงานของรัฐและภาคเอกชน

อย่างไรก็ตาม เนื่องจากทิศทางการพัฒนารัฐบาลดิจิทัล มุ่งเน้นในประเด็นสนับสนุนการเชื่อมโยงแลกเปลี่ยนข้อมูล เพื่อการบริการสาธารณะ (Public Services) ที่มีประชาชนเป็นศูนย์กลาง (Citizen Centric Government) โดยยกระดับการเปิดเผยข้อมูล (Open Data) เพื่อผูกพันภาครัฐในการส่งเสริมความโปร่งใสโดยให้อำนาจภาคประชาชน ต่อต้านการทุจริต รวมถึงการส่งเสริมการพัฒนาด้านเศรษฐกิจและสังคมเป็นหลัก ซึ่งการดำเนินการในลักษณะดังกล่าว แม้เป็นทิศทางที่เหมาะสมถูกต้อง แต่กลับลดโอกาสในการเชื่อมโยงหรือเปิดเผยข้อมูลในมิติงานด้านความมั่นคง ซึ่งมีทั้งหน่วยงานของรัฐและภาคเอกชนต่างเป็นเจ้าของข้อมูล เนื่องจากมีประเด็นความกังวลในการสนับสนุนการดำเนินการ ทั้งในแง่ขอบเขตหน้าที่และอำนาจตามกฎหมาย รวมถึงความรับผิดชอบในด้านต่าง ๆ เช่น การรักษาชั้นความลับ หรือผลที่อาจกระทบต่อการก้าวล่วงความเป็นส่วนบุคคลตามสิทธิและเสรีภาพที่ประชาชนทั่วไปพึงได้รับตามบทบัญญัติรัฐธรรมนูญแห่งราชอาณาจักรไทย [๖] และกฎหมายที่เกี่ยวข้อง เป็นต้น

๒.๓ ภารกิจงานบูรณาการข้อมูลของ กอ.รมน.

เพื่อให้เกิดการพัฒนากลไกการบูรณาการข้อมูลด้านความมั่นคง ในลักษณะเสริมสร้างควบคู่กับการพัฒนาการบูรณาการข้อมูลในมิติด้านเศรษฐกิจ สังคม และการบริการประชาชนตามที่กล่าวในข้างต้น นายกรัฐมนตรีในฐานะประธานสภาความมั่นคงแห่งชาติ ได้กำหนดความรับผิดชอบให้ กอ.รมน. เป็นหน่วยงานกลาง ระดับอำนวยการและประสานการปฏิบัติให้เกิดการเชื่อมโยงแลกเปลี่ยนข้อมูล รวมทั้งทำหน้าที่เป็นศูนย์กลางข้อมูลด้านความมั่นคง (Data Center) ของประเทศ โดยมีกฎหมาย แผนงาน และอนุมัติหลักการที่สำคัญ สรุปได้ดังนี้

๒.๓.๑ อำนาจและหน้าที่อำนวยการรักษาความมั่นคงภายในราชอาณาจักร

ภายใต้พระราชบัญญัติการรักษาความมั่นคงภายในราชอาณาจักร พ.ศ. ๒๕๕๑ [๗] ซึ่งได้กำหนดให้จัดตั้ง กอ.รมน. ขึ้นในสำนักนายกรัฐมนตรี มีอำนาจหน้าที่และรับผิดชอบเกี่ยวกับการรักษาความมั่นคงภายในราชอาณาจักร โดยมีนายกรัฐมนตรีในฐานะหัวหน้ารัฐบาล เป็นผู้อำนวยการรักษาความมั่นคงภายในราชอาณาจักร (ผอ.รมน.) ซึ่ง กอ.รมน. มีความจำเป็นต้องบูรณาการการเชื่อมโยงข้อมูลเกี่ยวข้องกับความมั่นคงระหว่างหน่วยงานของรัฐและภาคเอกชนที่เกี่ยวข้อง เพื่อนำไปใช้สนับสนุนการดำเนินงาน ตามอำนาจหน้าที่ที่ได้รับมอบหมาย ดังนี้

๒.๓.๑.๑ ติดตาม ตรวจสอบ และประเมินแนวโน้มของสถานการณ์ที่อาจก่อให้เกิดภัยคุกคามด้านความมั่นคงภายในราชอาณาจักร และรายงานคณะรัฐมนตรีเพื่อพิจารณาดำเนินการต่อไป

๒.๓.๑.๒ อำนวยการในการรักษาความมั่นคงภายในราชอาณาจักร โดยมีอำนาจหน้าที่เสนอแผนและแนวทางในการปฏิบัติงาน และดำเนินการต่อคณะรัฐมนตรีเพื่อพิจารณาให้ความเห็นชอบ เมื่อคณะรัฐมนตรีให้ความเห็นชอบแล้ว ให้หน่วยงานของรัฐปฏิบัติตามแผนและแนวทางนั้น

๒.๓.๑.๓ อำนวยการ ประสานงาน และเสริมการปฏิบัติของหน่วยงานของรัฐที่เกี่ยวข้องในการดำเนินการตามแผนและแนวทางในการปฏิบัติงานในข้อ ๒.๓.๑.๒ ในการนี้ คณะรัฐมนตรีจะมอบหมายให้ กอ.รมน. มีอำนาจในการกำกับการดำเนินการของหน่วยงานของรัฐตามที่คณะรัฐมนตรีกำหนดด้วยก็ได้

๒.๓.๑.๔ เสริมสร้างให้ประชาชนตระหนักในหน้าที่ที่ต้องพิทักษ์รักษาไว้ซึ่งชาติ ศาสนา และพระมหากษัตริย์ สร้างความรักความสามัคคีของคนในชาติ รวมทั้งส่งเสริมให้ประชาชนเข้ามามีส่วนร่วมในการป้องกันและแก้ไขปัญหาต่าง ๆ ที่กระทบต่อความมั่นคงภายในราชอาณาจักรและความสงบเรียบร้อยของสังคม

๒.๓.๑.๕ ดำเนินการอื่นตามที่กฎหมายบัญญัติหรือตามที่คณะรัฐมนตรี สภาความมั่นคงแห่งชาติหรือนายกรัฐมนตรีมอบหมาย

๒.๓.๒ กรอบความรับผิดชอบในฐานะศูนย์กลางข้อมูลด้านความมั่นคง

๒.๓.๒.๑ การกำหนดความรับผิดชอบ

ด้วย สมช. ได้จัดทำแผนปฏิบัติการด้านการบูรณาการข้อมูลด้านความมั่นคง ระยะที่ ๑ (พ.ศ. ๒๕๖๓ - ๒๕๖๕) [๘] โดยมีความมุ่งหมายเพื่อให้การบูรณาการข้อมูลสามารถนำไปสู่การปฏิบัติ รวมทั้งมีความประสานสอดคล้องเป็นไปในทิศทางเดียวกับยุทธศาสตร์ชาติ ๒๐ ปี แผนแม่บทภายใต้ยุทธศาสตร์ชาติประเด็นความมั่นคง ด้านการพัฒนากลไกการบริหารจัดการความมั่นคงแบบองค์รวม และนโยบายและแผนระดับชาติว่าด้วยความมั่นคงแห่งชาติ (พ.ศ. ๒๕๖๒ – ๒๕๖๕) โดยหน่วยงานของรัฐที่เกี่ยวข้อง ได้พิจารณาให้ความเห็นชอบ และนายกรัฐมนตรี/ประธานสภาความมั่นคงแห่งชาติ ได้กรุณาอนุมัติและให้ประกาศใช้แผนปฏิบัติการด้านดังกล่าว ตั้งแต่วันที่ ๒๗ ธันวาคม ๒๕๖๒

๒.๓.๒.๒ แนวทางการพัฒนาการบูรณาการข้อมูลด้านความมั่นคง

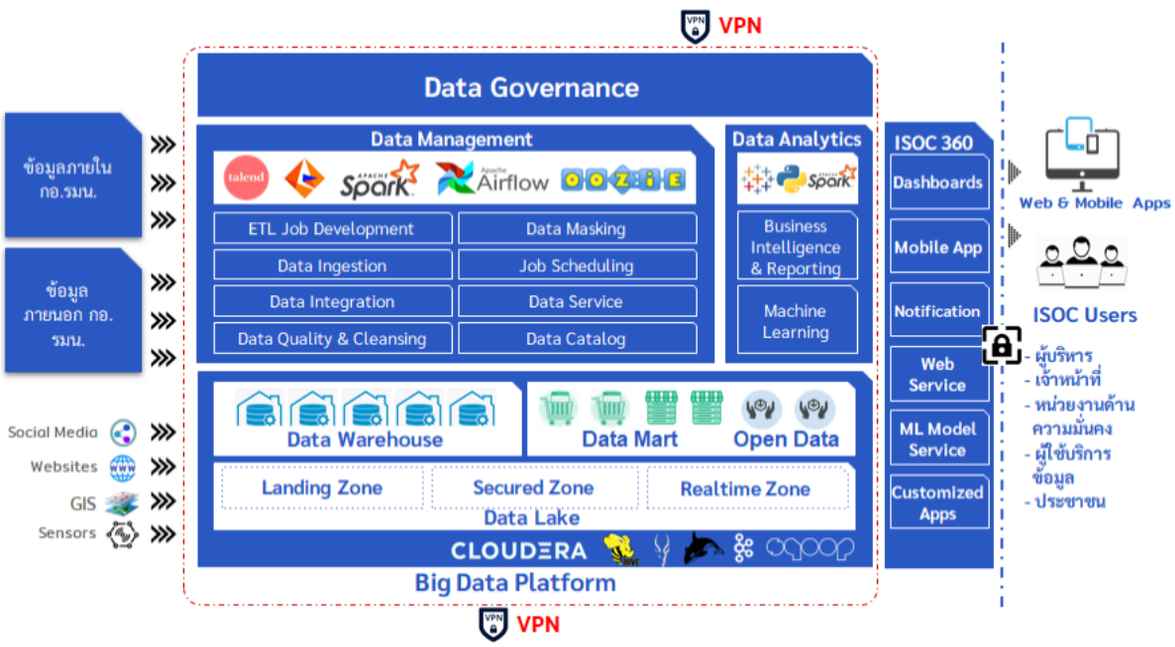
แผนปฏิบัติการด้านการบูรณาการข้อมูลด้านความมั่นคง ระยะที่ ๑ (พ.ศ. ๒๕๖๓ - ๒๕๖๕) ได้กำหนดแนวทางการพัฒนา แบ่งเป็น ๔ แนวทาง ดังนี้

๒.๓.๒.๒ (๑) นโยบายการบูรณาการฐานข้อมูล : มุ่งเน้นการศึกษา ทบทวน ปรับปรุง นโยบาย แผน กฎ ระเบียบ เพื่อกำหนดกรอบแนวทางดำเนินงานของหน่วยงานของรัฐที่เกี่ยวข้องกับฐานข้อมูล รวมทั้งเสริมสร้างและบูรณาการข้อมูลร่วมกันเพื่อสนับสนุนยุทธศาสตร์ชาติด้านความมั่นคง

๒.๓.๒.๒ (๒) การพัฒนาระบบฐานข้อมูล : มุ่งเน้นพัฒนาระบบฐานข้อมูลที่เหมาะสม โดยส่งเสริมการจัดทำประเภทบัญชีข้อมูล พัฒนาระบบเทคโนโลยีที่ทันสมัยให้กับหน่วยงานของรัฐที่มีหน้าที่ดำเนินการในกิจการงานความมั่นคง รวมทั้งพัฒนาและวางแผนระบบโครงสร้างอัตรากำลัง และศักยภาพของบุคลากรให้มีความรู้ความสามารถและความเชี่ยวชาญเฉพาะด้าน

๒.๓.๒.๒ (๓) การดำเนินงานด้านเทคนิคเพื่อบูรณาการข้อมูลระหว่างหน่วยงาน : ให้ความสำคัญกับการจัดทำบิ๊กดาต้าแพลตฟอร์มด้านความมั่นคง (ตามรูปที่ ๒) โดยพัฒนาระบบสารสนเทศเพื่อบริหารจัดการการเชื่อมโยงและแลกเปลี่ยนข้อมูลระหว่างหน่วยงานของรัฐและภาคเอกชน พัฒนาโครงสร้างพื้นฐานการจัดเก็บและระบบประมวลผลสำหรับการวิเคราะห์ข้อมูลขนาดใหญ่ และพัฒนาระบบรายการข้อมูลภาครัฐ (Government Data Catalog)

๒.๓.๒.๒ (๔) การบริหารจัดการแผนปฏิบัติการด้านการบูรณาการข้อมูลด้านความมั่นคง ระยะที่ ๑ (พ.ศ. ๒๕๖๓ - ๒๕๖๕) : กำหนดแนวทางขับเคลื่อนโดยมีทิศทางที่สอดคล้องกับ “แนวความคิดการบริหารจัดการยุทธศาสตร์ชาติด้านความมั่นคง” ซึ่งให้ความสำคัญกับการพัฒนากลไกการบริหารจัดการความมั่นคงแบบองค์รวม แผนแม่บทภายใต้ยุทธศาสตร์ชาติด้านความมั่นคง และสร้างกลไกความร่วมมือ/ข้อตกลงหรือการแลกเปลี่ยนและเชื่อมโยงข้อมูลระหว่างหน่วยงานของรัฐ ตลอดจนเสริมสร้างและพัฒนาองค์ความรู้เกี่ยวกับการมีข้อมูลและการบูรณาการ



รูปที่ ๒ โครงสร้างการพัฒนาบิ๊กดาต้าแพลตฟอร์มด้านความมั่นคง

๒.๓.๒.๓ การมอบหมายความรับผิดชอบ

แผนปฏิบัติการด้านการบูรณาการข้อมูลด้านความมั่นคง ระยะที่ ๑ (พ.ศ. ๒๕๖๓ - ๒๕๖๕) ได้แบ่งมอบความรับผิดชอบสนับสนุนการบูรณาการข้อมูล แบ่งเป็น ๓ ระดับ ดังนี้

๒.๓.๒.๓ (๑) ระดับนโยบาย : มอบหมายให้ สภาความมั่นคงแห่งชาติ (โดย สมช.) เป็นหน่วยรับผิดชอบ โดยแต่งตั้งคณะกรรมการบูรณาการฐานข้อมูล ซึ่งมีเลขาธิการ สมช. เป็นประธานกรรมการ มีหน้าที่กำหนดนโยบายและแนวทางการบูรณาการฐานข้อมูล และการบริหารจัดการแผนปฏิบัติการด้านการบูรณาการข้อมูลในระดับนโยบาย

๒.๓.๒.๓ (๒) ระดับอำนวยการ : มอบให้ กอ.รมน. ทำหน้าที่เป็นศูนย์กลางข้อมูลด้านความมั่นคง (Data Center) โดยนำเทคโนโลยีดิจิทัลสมัยใหม่ ได้แก่ บิ๊กดาต้าแพลตฟอร์ม ฯลฯ มาใช้เป็น

เครื่องมือสนับสนุนการดำเนินงาน และเป็นหน่วยงานกลางระดับอำนวยการและประสานการปฏิบัติเพื่อให้เกิดบูรณาการข้อมูล ตลอดจนเชื่อมโยงแลกเปลี่ยนข้อมูลกับหน่วยงานของรัฐ รวมทั้งศูนย์อำนวยการรักษาผลประโยชน์ของชาติทางทะเล (ศรชล.) และภาคเอกชน

๒.๓.๒.๓ (๓) ระดับปฏิบัติ : หน่วยงานของรัฐ ระดับกระทรวง/กรม ที่เกี่ยวข้อง รวมทั้ง ศรชล. เป็นหน่วยดำเนินการสนับสนุนข้อมูล โดยแลกเปลี่ยนเชื่อมโยงกับ กอ.รมน. (ศูนย์กลางข้อมูลด้านความมั่นคง) ตลอดจนจัดทำบัญชีข้อมูลของหน่วยงานของรัฐ เพื่อใช้สำหรับบูรณาการข้อมูลร่วมกับหน่วยงานที่เกี่ยวข้องต่อไป

๒.๔ สภาพแวดล้อมด้านกฎหมายและระเบียบที่เกี่ยวข้อง

กฎหมายและนโยบายที่มีความเกี่ยวข้องกับการบูรณาการข้อมูล และมีอิทธิพลต่อหลักแนวคิดการธรรมาภิบาลข้อมูลของ กอ.รมน. ในด้านต่าง ๆ สรุปได้ดังนี้

๒.๔.๑ ด้านการธรรมาภิบาลข้อมูล

๒.๔.๑.๑ พระราชบัญญัติการบริหารงานและการให้บริการภาครัฐผ่านระบบดิจิทัล พ.ศ. ๒๕๖๒ [๙] กำหนดให้หน่วยงานของรัฐจัดให้มีการบริหารงานภาครัฐและการจัดทำบริการสาธารณะเป็นไปด้วย ความสะดวก รวดเร็ว มีประสิทธิภาพ และตอบสนองต่อการให้บริการและการอำนวยความสะดวกแก่ประชาชน รวมทั้งจัดให้มีการบริหารจัดการและการบูรณาการข้อมูลภาครัฐ และการทำงานให้มีความสอดคล้องกันและเชื่อมโยงเข้าด้วยกันอย่างมั่นคงปลอดภัย โดยมีประเด็นสำคัญ ดังนี้

๒.๔.๑.๑ (๑) ให้มีคณะกรรมการพัฒนารัฐบาลดิจิทัล มีหน้าที่และอำนาจที่สำคัญ ได้แก่ การจัดทำ “ธรรมาภิบาลข้อมูลภาครัฐ” เพื่อเป็นหลักการและแนวทางในการดำเนินการ

๒.๔.๑.๑ (๒) ให้หน่วยงานของรัฐจัดทำ “ธรรมาภิบาลข้อมูลภาครัฐในระดับหน่วยงาน” และดำเนินการดังต่อไปนี้ให้เป็นไปตาม “ธรรมาภิบาลข้อมูลภาครัฐ” ในข้อ ๒.๔.๑.๑ (๑)

๒.๔.๑.๑ (๓) ให้หน่วยงานของรัฐ สนับสนุนข้อมูลดิจิทัลที่ได้พัฒนาขึ้นและครอบครองให้กับหน่วยงานของรัฐอื่น ตามที่ได้รับการร้องขอ เพื่อให้เกิดการบูรณาการการเชื่อมโยงแลกเปลี่ยนข้อมูลระหว่างกัน อันเป็นประโยชน์ในการบริหารราชการแผ่นดินและการให้บริการประชาชน

๒.๔.๑.๑ (๔) หน่วยงานของรัฐผู้รับข้อมูลดิจิทัล ตามข้อ ๒.๔.๑.๑ (๓) ต้องใช้ข้อมูลตามวัตถุประสงค์ในหน้าที่และอำนาจของหน่วยงานเท่านั้น และต้องดูแลรักษาข้อมูลให้มีความมั่นคงปลอดภัย ไม่มีการเปิดเผยหรือโอนข้อมูลไปยังบุคคลที่ไม่มีสิทธิเข้าถึงข้อมูล

๒.๔.๑.๑ (๕) ในกรณีที่หน่วยงานของรัฐ ประสงค์ใช้ข้อมูลส่วนบุคคลในรูปแบบข้อมูลดิจิทัล เพื่อประโยชน์ในการบริหารราชการแผ่นดิน หน่วยงานของรัฐนั้น สามารถขอเชื่อมโยงและแลกเปลี่ยนข้อมูลส่วนบุคคลนั้น จากหน่วยงานของรัฐที่ครอบครองข้อมูลดังกล่าว เพื่อนำมาวิเคราะห์หรือประมวลผลได้ (ภายใต้บทบัญญัติแห่งกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล)

๒.๔.๑.๒ ประกาศคณะกรรมการพัฒนารัฐบาลดิจิทัล เรื่อง ธรรมาภิบาลข้อมูลภาครัฐ [๑๐] : ให้หน่วยงานของรัฐจัดทำ “ธรรมาภิบาลข้อมูลภาครัฐในระดับหน่วยงาน” ให้สอดคล้องกับ “ธรรมาภิบาลข้อมูลภาครัฐ” ตามประกาศของคณะกรรมการฯ ประกอบด้วยเนื้อหาอย่างน้อย ดังนี้

๒.๔.๑.๒ (๑) การกำหนดสิทธิ หน้าที่ และความรับผิดชอบของผู้ซึ่งมีหน้าที่เกี่ยวข้องกับการบริหารจัดการข้อมูลของหน่วยงาน

๒.๔.๑.๒ (๒) การวางแผนการดำเนินงาน การปฏิบัติตามแผนการดำเนินงาน การตรวจสอบและการรายงานผลการดำเนินงาน และการปรับปรุงแผนการดำเนินงานอย่างต่อเนื่อง เพื่อให้ระบบบริหารและกระบวนการจัดการข้อมูลมีประสิทธิภาพสามารถเชื่อมโยง แลกเปลี่ยน และบูรณาการข้อมูลระหว่างกันทั้งภายในและภายนอกหน่วยงาน และคุ้มครองข้อมูลให้มีประสิทธิภาพ

๒.๔.๑.๒ (๓) การกำหนดมาตรการควบคุมและพัฒนาคุณภาพข้อมูล เพื่อให้ข้อมูลมีความถูกต้องครบถ้วน เป็นปัจจุบัน มั่นคงปลอดภัย และไม่ละเมิดความเป็นส่วนบุคคล รวมทั้งสามารถเชื่อมโยงแลกเปลี่ยน บูรณาการ และใช้ประโยชน์ได้อย่างมีประสิทธิภาพ

๒.๔.๑.๒ (๔) การวัดผลการบริหารจัดการข้อมูล โดยอย่างน้อยประกอบด้วยการประเมินความพร้อมของ “ธรรมาภิบาลข้อมูลภาครัฐในระดับหน่วยงาน” การประเมินคุณภาพข้อมูล และการประเมินความมั่นคงปลอดภัยของข้อมูล

๒.๔.๑.๒ (๕) การจำแนกหมวดหมู่ของข้อมูล เพื่อกำหนดนโยบายข้อมูลหรือกฎเกณฑ์เกี่ยวกับผู้มีสิทธิเข้าถึงและใช้ประโยชน์จากข้อมูลต่าง ๆ ภายในหน่วยงาน เพื่อให้ผู้ที่มีหน้าที่เกี่ยวข้องสามารถดำเนินการได้ตามนโยบายหรือแนวปฏิบัติได้อย่างถูกต้อง และสอดคล้องตามกฎหมายที่เกี่ยวข้อง อันจะนำไปสู่การบริหารจัดการข้อมูลภาครัฐอย่างเป็นระบบ

๒.๔.๑.๒ (๖) การจัดทำคำอธิบายชุดข้อมูลดิจิทัลของภาครัฐและบัญชีข้อมูลให้มีความถูกต้อง ครบถ้วน และเป็นปัจจุบัน

๒.๔.๒ ด้านการเปิดเผยข้อมูล

ภารกิจการบูรณาการข้อมูลของ กอ.รมน. จำเป็นต้องประสานหน่วยงานของรัฐและภาคเอกชนสนับสนุนการเปิดเผยข้อมูล และเชื่อมโยงแลกเปลี่ยนเข้ามายังศูนย์กลางข้อมูลด้านความมั่นคง รวมทั้งการเปิดเผยข้อมูลจากศูนย์กลางข้อมูลด้านความมั่นคง ให้กับหน่วยงานของรัฐ ภาคเอกชน หรือประชาชน โดยมีกฎหมายและระเบียบที่เกี่ยวข้อง ดังนี้

๒.๔.๒.๑ รัฐธรรมนูญแห่งราชอาณาจักรไทย พ.ศ. ๒๕๖๐ [๖] กำหนดให้รัฐต้องเปิดเผยข้อมูลหรือข่าวสารสาธารณะในครอบครองของหน่วยงานของรัฐ ที่มิใช่ข้อมูลเกี่ยวกับความมั่นคงของรัฐ หรือเป็นความลับของทางราชการตามที่กฎหมายบัญญัติ และต้องจัดให้ประชาชนเข้าถึงข้อมูลหรือข่าวสารดังกล่าวได้โดยสะดวก

๒.๔.๒.๒ พระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ. ๒๕๔๐ [๑๑] เป็นกฎหมายที่ให้ความสำคัญกับการเปิดเผยข้อมูล ความโปร่งใส การมีส่วนร่วมของประชาชน ซึ่งเป็นไปตามหลักธรรมาภิบาล เพื่อให้การดำเนินการของรัฐมีประสิทธิภาพและประสิทธิผล รวมทั้ง ให้ความสำคัญกับความรับผิดชอบต่อการปฏิบัติหน้าที่ราชการ โดยใช้หลักการ (๑) เปิดเผยเป็นหลัก ปกปิดเป็นข้อยกเว้น (๒) ผู้ขอมีสิทธิรับรู้โดยไม่จำเป็นต้องมีส่วนได้เสีย และ (๓) ให้ความคุ้มครองข้อมูลส่วนบุคคล โดยมีประเด็นที่หน่วยงานของรัฐต้องดำเนินการ สรุปได้ดังนี้

๒.๔.๒.๒ (๑) ห้ามมิให้เปิดเผยข้อมูลข่าวสารของราชการที่อาจก่อให้เกิดความเสียหายต่อสถาบันพระมหากษัตริย์

๒.๔.๒.๒ (๒) ให้กำหนดวิธีการคุ้มครองข้อมูลข่าวสาร เพื่อให้เกิดความชัดเจนในทางปฏิบัติว่าข้อมูลข่าวสารของทางราชการ มีวิธีรักษาป้องกันมิให้รั่วไหล สามารถเปิดเผยต่อบุคคลใดได้หรือไม่ ภายใต้เงื่อนไขเช่นใด โดยต้องเป็นไปตามตามระเบียบที่คณะรัฐมนตรีกำหนดว่าด้วยการรักษาความลับของทางราชการ

๒.๔.๒.๒ (๓) จัดให้มีระบบจัดเก็บข้อมูลข่าวสารส่วนบุคคลเท่าที่เกี่ยวข้องและยกเลิกเมื่อหมดความจำเป็น โดยพยายามเก็บข้อมูลข่าวสารโดยตรงจากเจ้าของข้อมูลส่วนบุคคล และแก้ไขให้ถูกต้องเสมอ รวมทั้ง ต้องจัดระบบรักษาความปลอดภัย เพื่อไม่ให้นำไปใช้อย่างไม่เหมาะสม

๒.๔.๒.๒ (๔) ห้ามมิให้เปิดเผยข้อมูลข่าวสารส่วนบุคคลต่อหน่วยงานของรัฐแห่งอื่นหรือผู้อื่น โดยปราศจากความยินยอมเป็นหนังสือของเจ้าของข้อมูลส่วนบุคคลที่ให้ไว้ล่วงหน้าหรือในขณะนั้น เว้นแต่เป็นการเปิดเผย ดังต่อไปนี้

๒.๔.๒.๒ (๔.๑) ต่อเจ้าหน้าที่รัฐภายในหน่วยงาน เพื่อนำไปใช้ตามอำนาจหน้าที่ของหน่วยงานของรัฐแห่งนั้น

๒.๔.๒.๒ (๔.๒) เป็นการใช้ข้อมูลตามปกติภายในวัตถุประสงค์ของการจัดเก็บข้อมูลข่าวสารส่วนบุคคล

๒.๔.๒.๒ (๔.๓) ต่อหน่วยงานที่ทำงานด้านแผน การสถิติ และสำมะโนต่าง ๆ ซึ่งมีหน้าที่ต้องรักษาข้อมูลข่าวสารส่วนบุคคลไว้ ไม่ให้เปิดเผยต่อไปยังผู้อื่น

๒.๔.๒.๒ (๔.๔) ต่อเจ้าหน้าที่ของรัฐ เพื่อป้องกันการฝ่าฝืนหรือไม่ปฏิบัติตามกฎหมาย การสืบสวน การสอบสวน หรือการฟ้องคดี ไม่ว่าเป็นคดีประเภทใดก็ตาม

๒.๔.๒.๒ (๔.๕) เป็นการให้ซึ่งจำเป็น เพื่อป้องกัน หรือระงับอันตรายต่อชีวิตหรือสุขภาพของบุคคล

๒.๔.๒.๒ (๔.๖) ต่อศาล และเจ้าหน้าที่ของรัฐ หรือหน่วยงานของรัฐหรือบุคคลที่มีอำนาจตามกฎหมาย ที่จะขอข้อเท็จจริงดังกล่าว

๒.๔.๒.๒ (๔.๗) กรณีอื่นตามที่กำหนดไว้ในพระราชกฤษฎีกา

๒.๔.๒.๓ พระราชบัญญัติข่าวกรองแห่งชาติ พ.ศ. ๒๕๖๒ [๑๒] ได้กำหนดให้สำนักข่าวกรองแห่งชาติ (สขช.) มีหน้าที่และอำนาจ ดังต่อไปนี้

๒.๔.๒.๓ (๑) ปฏิบัติงานเกี่ยวกับกิจการการข่าวกรอง การต่อต้านข่าวกรอง การข่าวกรองทางการสื่อสารและการรักษาความปลอดภัยฝ่ายพลเรือน

๒.๔.๒.๓ (๒) ติดตามสถานการณ์ภายในประเทศและต่างประเทศที่มีผลกระทบต่อความมั่นคงแห่งชาติและรายงานต่อนายกรัฐมนตรีและสภาความมั่นคงแห่งชาติ

๒.๔.๒.๓ (๓) กระจายข่าวกรองที่มีผลกระทบต่อความมั่นคงแห่งชาติให้หน่วยงานของรัฐหรือรัฐวิสาหกิจที่เกี่ยวข้องใช้ประโยชน์ตามความเหมาะสม

๒.๔.๒.๓ (๔) จะเปิดเผยบรรดาข้อมูลข่าวสารที่ สขช. ได้รับมาเนื่องจากการปฏิบัติหน้าที่ตามพระราชบัญญัติฯ มิได้ เว้นแต่เป็นการเปิดเผยต่อหน่วยข่าวกรอง หน่วยงานความมั่นคง นายกรัฐมนตรี หรือตามคำสั่งศาล

๒.๔.๓ ด้านการรักษาความลับและความปลอดภัย

การบูรณาการข้อมูล มีองค์ประกอบข้อมูลทั้งที่เป็นข้อมูลข่าวสารทั่วไป และข้อมูลข่าวสารที่มีระดับชั้นความลับ ซึ่งจำเป็นต้องมีการรักษาความปลอดภัยบุคคล เอกสาร สถานที่ ให้เป็นไปตามกฎหมายและระเบียบที่เกี่ยวข้องกำหนด อย่างเคร่งครัด ดังนี้

๒.๔.๓.๑ ระเบียบว่าด้วยการรักษาความลับของทางราชการ พ.ศ. ๒๕๕๔ และที่แก้ไขเพิ่มเติม [๑๓,๑๔] ได้การกำหนดนิยาม หลักเกณฑ์ และวิธีการในการรักษาความลับในส่วนที่เกี่ยวข้องกับการบูรณาการข้อมูล สรุปได้ดังนี้

๒.๔.๓.๑ (๑) กำหนดประเภทชั้นความลับ แบ่งเป็น ๓ ระดับ

๒.๔.๓.๑ (๑.๑) ชั้นลับที่สุด หมายความถึง ข้อมูลข่าวสารลับซึ่งหากเปิดเผยทั้งหมด หรือเพียงบางส่วนจะก่อให้เกิดความเสียหายแก่ประโยชน์แห่งรัฐอย่างร้ายแรงที่สุด

๒.๔.๓.๑ (๑.๒) ชั้นลับมาก หมายความถึง ข้อมูลข่าวสารลับซึ่งหากเปิดเผยทั้งหมด หรือเพียงบางส่วนจะก่อให้เกิดความเสียหายแก่ประโยชน์แห่งรัฐอย่างร้ายแรง

๒.๔.๓.๑ (๑.๓) ชั้นลับ หมายความถึง ข้อมูลข่าวสารลับ ซึ่งหากเปิดเผยทั้งหมด หรือเพียงบางส่วนจะก่อให้เกิดความเสียหายแก่ประโยชน์แห่งรัฐ

๒.๔.๓.๑ (๒) กำหนดนิยาม “ข้อมูลข่าวสารลับ” หมายถึง ข้อมูลข่าวสารที่มีคำสั่งไม่ให้เปิดเผย และอยู่ในความครอบครองหรือควบคุมดูแลของหน่วยงานของรัฐ ไม่ว่าจะเป็นเรื่องที่เกี่ยวกับการดำเนินงานของรัฐหรือที่เกี่ยวกับเอกชน ซึ่งมีการกำหนดให้มีชั้นความลับเป็น ชั้นลับ ชั้นลับมาก หรือชั้นลับที่สุด โดยคำถึงถึงการปฏิบัติหน้าที่ของหน่วยงานของรัฐและประโยชน์แห่งรัฐ ประกอบกัน

๒.๔.๓.๑ (๓) การโอนข้อมูลข่าวสารลับระหว่างหน่วยงานของรัฐหรือการโอนภายในหน่วยงานเดียวกัน ให้เจ้าหน้าที่ผู้โอนและเจ้าหน้าที่ผู้รับโอนจัดทำบันทึกการโอนและการรับโอนข้อมูลข่าวสารลับตามแบบที่นายกรัฐมนตรีกำหนดโดยประกาศในราชกิจจานุเบกษาไว้เป็นหลักฐานและให้นายทะเบียนข้อมูลข่าวสารลับจดแจ้งการโอนข้อมูลข่าวสารลับดังกล่าวไว้ในทะเบียนควบคุมข้อมูลข่าวสารลับด้วย

๒.๔.๓.๑ (๔) การให้ยืมข้อมูลข่าวสารลับ ให้หัวหน้าหน่วยงานของรัฐหรือผู้ซึ่งหัวหน้าหน่วยงานของรัฐมอบหมายพิจารณาด้วยว่า ผู้ยืมมีหน้าที่ดำเนินการในเรื่องที่ยืมและสามารถปฏิบัติตามระเบียบฯ ได้หรือไม่ และหากเรื่องที่ผู้ประสงค์จะขอยืมเป็นเรื่องที่หน่วยงานของรัฐอื่นเป็นหน่วยงานเจ้าของเรื่อง การให้ยืมต้องได้รับอนุญาตจากหน่วยงานเจ้าของเรื่องนั้นก่อน เว้นแต่ผู้ยืมจะเป็นหน่วยงานเจ้าของเรื่องนั้นเอง ทั้งนี้ ให้นายทะเบียนข้อมูลข่าวสารลับ ทำบันทึกการยืมพร้อมทั้งจดแจ้งการยืมไว้ในทะเบียนควบคุมข่าวสารลับด้วย

๒.๔.๓.๑ (๕) หัวหน้าหน่วยงานของรัฐ จะสั่งทำลายข้อมูลข่าวสารลับได้ต่อเมื่อส่งข้อมูลข่าวสารลับให้หอจดหมายเหตุแห่งชาติ พิจารณาก่อนว่าไม่มีคุณค่าในการเก็บรักษา ยกเว้นในกรณีที่การเก็บรักษา

ข้อมูลข่าวสารลับประเภท “ชั้นลับที่สุด” มีความเสี่ยงต่อการรั่วไหลอันจะก่อให้เกิดอันตรายแก่ประโยชน์แห่งรัฐ ให้หัวหน้าหน่วยงานของรัฐ พิจารณาแล้วเห็นว่ามีความจำเป็นอย่างยิ่งที่จะต้องทำลาย ให้สั่งทำลายข้อมูลข่าวสารลับ ชั้นลับที่สุดนั้นได้

๒.๔.๓.๑ (๖) ให้หน่วยงานของรัฐ จัดให้มีแผนการปฏิบัติในเวลาฉุกเฉิน โดยมีแผนการเคลื่อนย้าย แผนการพิทักษ์รักษา และแผนการทำลายข้อมูลข่าวสารลับ เพื่อนำมาปฏิบัติเป็นลำดับชั้นตามความรุนแรงของสถานการณ์

๒.๔.๓.๑ (๗) ในกรณีที่ข้อมูลข่าวสารลับสูญหาย ให้ผู้ทราบข้อเท็จจริง รายงานข้อเท็จจริงที่เกี่ยวข้อง ให้หัวหน้าหน่วยงานของรัฐที่ตนสังกัดทราบ เพื่อดำเนินการต่อไป และให้นายทะเบียนข้อมูลข่าวสารลับบันทึกการที่ข้อมูลข่าวสารลับลับสูญหายไว้ในทะเบียนควบคุมข้อมูลข่าวสารลับ

๒.๔.๓.๒ ระเบียบสำนักนายกรัฐมนตรีว่าด้วยการรักษาความปลอดภัยแห่งชาติ พ.ศ. ๒๕๕๒ และที่แก้ไขเพิ่มเติม [๑๕, ๑๖] ได้วางกรอบแนวทางปฏิบัติ เพื่อพิทักษ์รักษาและคุ้มครองป้องกันสิ่งที่เป็นความลับของทางราชการ ซึ่งรวมถึงข้อมูลข่าวสารลับ ตลอดจนหน่วยงานของรัฐ เจ้าหน้าที่ของรัฐ และทรัพย์สินมีค่าของแผ่นดิน ให้พ้นจากการรั่วไหล การจารกรรม การก่อวินาศกรรม การบ่อนทำลาย การก่อการร้าย การกระทำที่เป็นภัยต่อความมั่นคง และผลประโยชน์แห่งรัฐ และการกระทำอื่นใดที่เป็นการเปิดเผยสิ่งที่เป็นความลับของทางราชการ ทั้งนี้มีประเด็นสำคัญสรุปได้ดังนี้

๒.๔.๓.๒ (๑) การรักษาความปลอดภัยแห่งชาติในส่วนที่เกี่ยวข้องกับข้อมูลข่าวสาร นอกจากต้องปฏิบัติตามที่กำหนดไว้ในระเบียบฯ แล้ว ให้เป็นไปตามระเบียบว่าด้วยการรักษาความลับของทางราชการ พ.ศ. ๒๕๕๔ และในกรณีการรักษาความปลอดภัยระบบเครือข่ายคอมพิวเตอร์และเทคโนโลยีสารสนเทศ ให้ถือปฏิบัติตามกฎหมาย กฎ ระเบียบ ประกาศ ข้อบังคับ คำสั่ง มติคณะรัฐมนตรีที่เกี่ยวกับหลักเกณฑ์และมาตรการรักษาความปลอดภัยด้านสารสนเทศด้วย

๒.๔.๓.๒ (๒) ให้หัวหน้าหน่วยงานของรัฐดำเนินการรักษาความปลอดภัยเกี่ยวกับสถานที่ โดยกำหนดมาตรการเพื่อพิทักษ์รักษาให้ความปลอดภัยแก่ที่สงวน อาคาร และสถานที่ของหน่วยงานของรัฐ ตลอดจนข้อมูลข่าวสาร วัสดุอุปกรณ์ ศูนย์ข้อมูลสารสนเทศ ระบบสาธารณูปโภค เจ้าหน้าที่ของรัฐ และสิ่งอื่นที่หัวหน้าหน่วยงานของรัฐกำหนด ที่อยู่ในอาคารและสถานที่ดังกล่าว ทั้งนี้รวมถึงข้อมูลข่าวสาร ศูนย์ข้อมูลสารสนเทศ และสิ่งอื่นซึ่งมิได้อยู่ภายในอาคารและสถานที่ของหน่วยงานของรัฐ โดยคำนึงถึงความจำเป็นแก่การปฏิบัติภารกิจของหน่วยงานของรัฐ

๒.๔.๓.๒ (๓) ให้เจ้าหน้าที่ของรัฐผู้พบเห็น หรือทราบ หรือสงสัยว่าจะมี หรือมีการละเมิดมาตรการรักษาความปลอดภัย ซึ่งรวมถึงความปลอดภัยทางระบบเครือข่ายคอมพิวเตอร์และเทคโนโลยีสารสนเทศด้วย รีบดำเนินการเบื้องต้นเพื่อลดความเสียหายให้เหลือน้อยที่สุดและรายงานผู้บังคับบัญชาทราบโดยเร็วที่สุด หรือให้แจ้งเจ้าหน้าที่ควบคุมการรักษาความปลอดภัย หรือเจ้าหน้าที่ผู้รับผิดชอบ เพื่อให้ประสานหน่วยงานของรัฐที่รับผิดชอบโดยตรง หรือหน่วยงานเอกชนที่ได้รับมอบหมายหรือเป็นคู่สัญญากับหน่วยงานของรัฐ ดำเนินการในทันทีที่เผชิญเหตุ

๒.๔.๓.๒ (๔) ให้หัวหน้าหน่วยงานของรัฐ มีหน้าที่ในการรักษาความปลอดภัยในหน่วยงานของตน ในกรณีที่หน่วยงานของรัฐ ได้มอบหมายหรือทำสัญญาว่าจ้างให้บุคคลภายนอกดำเนินการ

อย่างหนึ่งอย่างใด ให้หัวหน้าหน่วยงานของรัฐกำกับดูแลผู้ได้รับมอบหมายหรือผู้เป็นคู่สัญญาซึ่งเป็นบุคคลภายนอกดังกล่าว ให้ต้องปฏิบัติในการรักษาความปลอดภัยแห่งชาติตามระเบียบฯ ด้วย

๒.๔.๔ ด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

ด้วยภารกิจการบูรณาการข้อมูลของ กอ.รมน. จำเป็นต้องดำเนินการผ่านระบบเครือข่ายคอมพิวเตอร์ที่ใช้เทคโนโลยีดิจิทัลขั้นสูง สนับสนุนการเชื่อมโยงแลกเปลี่ยน จัดเก็บ วิเคราะห์ ประมวลผลข้อมูลขนาดใหญ่ และนำเสนอในรูปแบบการจัดทำรายงานอย่างเป็นระบบ ดังนั้น กอ.รมน. จึงจำเป็นต้องดำเนินการให้เป็นไปตามพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ [๑๗] ดังนี้

๒.๔.๔.๑ จัดทำประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของหน่วยงาน ประกอบด้วย (๑) แผนการตรวจสอบและประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ และ (๒) แผนการรับมือภัยคุกคามทางไซเบอร์ ที่มีความสอดคล้องกับนโยบายและแผนว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ตามที่คณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติกำหนด

๒.๔.๔.๒ ป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ตามประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของหน่วยงาน และจะต้องดำเนินการให้เป็นไปตามประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ตามที่คณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์กำหนด

๒.๔.๔.๓ จัดให้มีการประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์โดยมีผู้ตรวจประเมิน รวมทั้งตรวจสอบด้านความมั่นคงปลอดภัยไซเบอร์ โดยผู้ตรวจสอบด้านความมั่นคงปลอดภัยสารสนเทศ (โดยผู้ตรวจสอบภายในหรือโดยผู้ตรวจสอบอิสระภายนอก) อย่างน้อยปีละ ๑ ครั้ง

๒.๔.๕ ด้านการคุ้มครองข้อมูลส่วนบุคคล

แม้ว่าพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ [๑๘] อาจไม่มีผลบังคับใช้ในกรณีการดำเนินการของหน่วยงานของรัฐที่มีหน้าที่ในการรักษาความมั่นคงของรัฐ หรือการรักษาความปลอดภัยของประชาชน แต่ กอ.รมน. ควรพิจารณานำบทบัญญัติมาใช้ประกอบการดำเนินการตามวัตถุประสงค์และนัยยะสำคัญของกฎหมาย เพื่อบังคับแก่การเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล ทั้งนี้ ในกรณีหน่วยงานของรัฐที่ควบคุมข้อมูลส่วนบุคคล ผู้ประมวลผลข้อมูลส่วนบุคคล หรือผู้ใช้งานข้อมูลส่วนบุคคล อยู่ในราชอาณาจักร (ไม่ว่าการเก็บรวบรวม ใช้ หรือเปิดเผยนั้น ได้กระทำภายในหรือนอกราชอาณาจักรก็ตาม) โดยมีประเด็นสำคัญที่เกี่ยวข้องกับการบูรณาการข้อมูล ดังนี้

๒.๔.๕.๑ หน่วยงานของรัฐที่ควบคุมข้อมูลส่วนบุคคล จะกระทำการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลไม่ได้หากเจ้าของข้อมูลส่วนบุคคลไม่ได้ให้ความยินยอมไว้ก่อนหรือในขณะนั้น เว้นแต่บทบัญญัติแห่งพระราชบัญญัตินี้หรือกฎหมายอื่นบัญญัติให้กระทำได้

๒.๔.๕.๒ หน่วยงานของรัฐที่ควบคุมข้อมูลส่วนบุคคล จะต้องแจ้งให้เจ้าของข้อมูลส่วนบุคคลทราบก่อนหรือในขณะเก็บรวบรวมข้อมูลส่วนบุคคล ถึงรายละเอียด ดังต่อไปนี้

๒.๔.๕.๒ (๑) วัตถุประสงค์ของการเก็บรวบรวม เพื่อการนำข้อมูลส่วนบุคคลไปใช้หรือเปิดเผย

๒.๔.๕.๒ (๒) ข้อมูลส่วนบุคคลที่จะมีการเก็บรวบรวมและระยะเวลาในการเก็บรวบรวมไว้ ทั้งนี้ ในกรณีที่ไม่สามารถกำหนดระยะเวลาดังกล่าวได้ชัดเจน ให้กำหนดระยะเวลาที่อาจคาดหมายได้ตามมาตรฐานของการเก็บรวบรวม

๒.๔.๕.๒ (๓) ประเภทของบุคคลหรือหน่วยงานซึ่งข้อมูลส่วนบุคคลที่เก็บรวบรวมอาจจะถูกเปิดเผย

๒.๔.๕.๒ (๔) ข้อมูลเกี่ยวกับผู้ควบคุมข้อมูลส่วนบุคคล สถานที่ติดต่อ และวิธีการติดต่อในกรณีที่มีตัวแทนหรือเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล ให้แจ้งข้อมูล สถานที่ติดต่อ และวิธีการติดต่อของตัวแทนหรือเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลด้วย

๒.๔.๕.๒ (๕) สิทธิของเจ้าของข้อมูลส่วนบุคคลตามกฎหมายที่เกี่ยวข้อง

๒.๔.๕.๓ การเก็บรวบรวมข้อมูลส่วนบุคคล ให้เก็บรวบรวมได้เท่าที่จำเป็นภายใต้วัตถุประสงค์อันชอบด้วยกฎหมายของหน่วยงานของรัฐที่ควบคุมข้อมูลส่วนบุคคล

๒.๔.๕.๔ หน่วยงานของรัฐที่ควบคุมข้อมูลส่วนบุคคล ต้องดำเนินการให้ข้อมูลส่วนบุคคลนั้นถูกต้องเป็นปัจจุบัน สมบูรณ์ และไม่ก่อให้เกิดความเข้าใจผิด

๒.๔.๕.๕ หน่วยงานของรัฐที่ควบคุมข้อมูลส่วนบุคคล มีหน้าที่สำคัญดังต่อไปนี้

๒.๔.๕.๕ (๑) จัดให้มีมาตรการรักษาความมั่นคงปลอดภัยที่เหมาะสม เพื่อป้องกันการสูญหาย เข้าถึง ใช้เปลี่ยนแปลง แก้ไข หรือเปิดเผยข้อมูลส่วนบุคคล โดยปราศจากอำนาจหรือโดยมิชอบ และต้องทบทวนมาตรการดังกล่าวเมื่อมีความจำเป็นหรือเมื่อเทคโนโลยีเปลี่ยนแปลงไป เพื่อให้มีประสิทธิภาพในการรักษาความมั่นคงปลอดภัยที่เหมาะสม

๒.๔.๕.๕ (๒) ในกรณีที่ต้องให้ข้อมูลส่วนบุคคลแก่บุคคลหรือนิติบุคคลอื่นที่ไม่ใช่ผู้ควบคุมข้อมูลส่วนบุคคล ต้องดำเนินการเพื่อป้องกันมิให้ผู้นั้นใช้หรือเปิดเผยข้อมูลส่วนบุคคล โดยปราศจากอำนาจหรือโดยมิชอบ

๒.๔.๕.๕ (๓) จัดให้มีระบบการตรวจสอบเพื่อดำเนินการลบหรือทำลายข้อมูลส่วนบุคคลเมื่อพ้นกำหนดระยะเวลาการเก็บรักษา หรือที่ไม่เกี่ยวข้องหรือเกินความจำเป็นตามวัตถุประสงค์ในการเก็บรวบรวมข้อมูลส่วนบุคคลนั้น หรือตามที่เจ้าของข้อมูลส่วนบุคคลร้องขอ หรือที่เจ้าของข้อมูลส่วนบุคคลได้ถอนความยินยอม

๒.๔.๕.๕ (๔) ให้หน่วยงานของรัฐที่ควบคุมข้อมูลส่วนบุคคล บันทึกรายการเพื่อให้เจ้าของข้อมูลส่วนบุคคลและสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล สามารถตรวจสอบได้

๒.๔.๕.๕ (๔.๑) ข้อมูลส่วนบุคคลที่มีการเก็บรวบรวม

๒.๔.๕.๕ (๔.๒) วัตถุประสงค์ของการเก็บรวบรวมข้อมูลส่วนบุคคลแต่ละประเภท

๒.๔.๕.๕ (๔.๓) ข้อมูลเกี่ยวกับหน่วยงานของรัฐที่ควบคุมข้อมูลส่วนบุคคล

๒.๔.๕.๕ (๔.๔) ระยะเวลาการเก็บรักษาข้อมูลส่วนบุคคล

๒.๔.๕.๕ (๔.๕) สิทธิและวิธีการเข้าถึงข้อมูลส่วนบุคคล รวมทั้งเงื่อนไขเกี่ยวกับบุคคลที่มีสิทธิเข้าถึงข้อมูลส่วนบุคคลและเงื่อนไขในการเข้าถึงข้อมูลส่วนบุคคลนั้น

๒.๔.๕.๕ (๔.๖) การใช้หรือเปิดเผยข้อมูลส่วนบุคคล ในกรณีที่หน่วยงานของรัฐที่ควบคุมข้อมูลส่วนบุคคล ใช้หรือเปิดเผยข้อมูลส่วนบุคคลที่ได้รับยกเว้นไม่ต้องขอความยินยอมตามเงื่อนไขที่กฎหมายกำหนด

๒.๔.๕.๕ (๔.๗) คำอธิบายเกี่ยวกับมาตรการรักษาความมั่นคงปลอดภัย

๒.๔.๕.๖ หน่วยงานของรัฐที่ใช้งานข้อมูลส่วนบุคคลมีหน้าที่ ดังต่อไปนี้

๒.๔.๕.๖ (๑) ดำเนินการเกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลตามคำสั่งที่ได้รับจากหน่วยงานของรัฐที่ควบคุมข้อมูลส่วนบุคคลเท่านั้น เว้นแต่คำสั่งนั้นขัดต่อกฎหมายหรือบทบัญญัติในการคุ้มครองข้อมูลส่วนบุคคลตามที่กฎหมายกำหนด

๒.๔.๕.๖ (๒) จัดให้มีมาตรการรักษาความมั่นคงปลอดภัยที่เหมาะสม เพื่อป้องกันการสูญหาย เข้าถึง ใช้ เปลี่ยนแปลง แก้ไข หรือเปิดเผยข้อมูลส่วนบุคคลโดยปราศจากอำนาจหรือโดยมิชอบ รวมทั้งแจ้งให้หน่วยงานของรัฐที่ควบคุมข้อมูลส่วนบุคคล ทราบถึงเหตุการละเมิดข้อมูลส่วนบุคคลที่เกิดขึ้น

๒.๔.๕.๖ (๓) จัดทำและเก็บรักษาบันทึกรายการของกิจกรรมการใช้งานข้อมูลส่วนบุคคลไว้ตามหลักเกณฑ์และวิธีการที่คณะกรรมการคุ้มครองข้อมูลส่วนบุคคลกำหนด

ในบทนี้ ได้สรุปข้อมูลความสำคัญประกอบการพิจารณาการวางระบบบริหารจัดการบูรณาการข้อมูลของ กอ.รมน. โดยมีเป้าประสงค์เพื่อให้สามารถนำไปวิเคราะห์ประมวลผล และนำข้อมูลไปใช้ประกอบการขับเคลื่อนการป้องกันและแก้ไขปัญหาด้านความมั่นคงในภาพรวมของประเทศ ผ่านกลไกการบริหารจัดการความมั่นคงแบบองค์รวมร่วมกับ สมช. และหน่วยงานของรัฐอื่น ๆ ภายใต้กรอบแนวคิดการเปลี่ยนผ่านไปสู่ “องค์กรที่ขับเคลื่อนด้วยข้อมูล (Data Driven Organization)” ทั้งนี้ เพื่อให้การดำเนินการเป็นไปด้วยความเรียบร้อย กอ.รมน. ในฐานะหน่วยระดับอำนวยการในการบูรณาการและประสานการปฏิบัติในการป้องกันและแก้ไขปัญหาความมั่นคงตามภารกิจที่กำหนดในพระราชบัญญัติการรักษาความมั่นคงภายในราชอาณาจักร พ.ศ. ๒๕๕๑ และในฐานะศูนย์กลางข้อมูลด้านความมั่นคงของประเทศ จำเป็นต้องยึดถือปฏิบัติตามกฎหมายและระเบียบที่เกี่ยวข้องทั้งในด้านธรรมาภิบาลข้อมูล เพื่อให้มีการบริหารจัดการข้อมูลที่ดี โปร่งใส น่าเชื่อถือ และตรวจสอบได้ โดยมีการควบคุมการเปิดเผยข้อมูล การเชื่อมโยงแลกเปลี่ยนข้อมูล การรักษาความลับของข้อมูลข่าวสาร การคุ้มครองข้อมูลส่วนบุคคล การรักษาความปลอดภัย ทั้งบุคคล เอกสาร สถานที่ รวมถึงระบบเครือข่ายคอมพิวเตอร์และเทคโนโลยีสารสนเทศ และการรักษาความมั่นคงปลอดภัยไซเบอร์ที่เกี่ยวข้อง อย่างเป็นระบบอีกด้วย

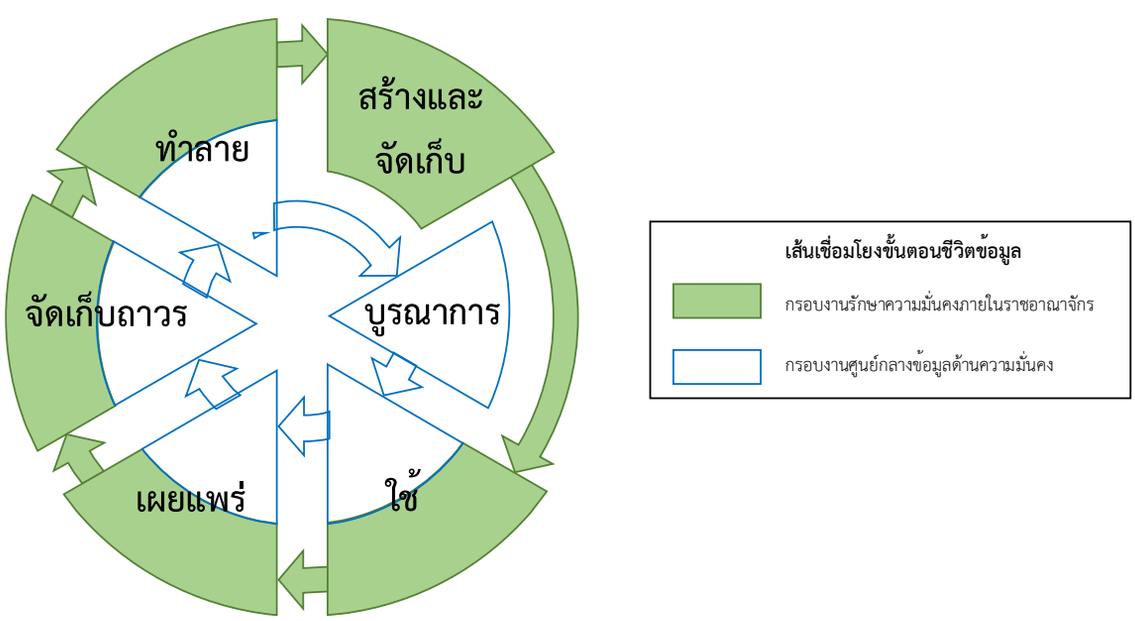
บทที่ ๓
หลักการธรรมาภิบาลข้อมูลของ กอ.รมน.

๓.๑ กล่าวนำ

ด้วยบทบาทและหน้าที่ในการบริหารจัดการการเชื่อมโยงแลกเปลี่ยน บูรณาการ วิเคราะห์ประมวลผล และเผยแพร่หรือเปิดเผยข้อมูล ภายใต้กรอบนโยบายและกฎหมายที่เกี่ยวข้องตามที่ได้สรุปในบทที่ ๒ จึงได้จัดทำธรรมาภิบาลข้อมูลด้านความมั่นคง กอ.รมน. เพื่อให้มีกรอบพื้นฐานในการบริหารจัดการ “ข้อมูล” ให้ดี มีความชัดเจน โปร่งใส ปลอดภัย และตรวจสอบได้ รวมทั้งมีการปรับปรุงพัฒนาให้มีความเหมาะสม สอดคล้องกับสถานการณ์ในแต่ละห้วงเวลา โดยในบทที่ ๓ นี้ เป็นการกล่าวสรุปรายละเอียดที่ใช้เป็น “หลัก” ในการจัดทำธรรมาภิบาลข้อมูล ทั้งในด้านนิยามของ วงจรชีวิตข้อมูล การบริหารจัดการข้อมูล ขอบเขตงานบูรณาการข้อมูล และวงรอบธรรมาภิบาลข้อมูลของ กอ.รมน. ตามลำดับ

๓.๒ วงจรชีวิตข้อมูล

เป้าหมายของการธรรมาภิบาลข้อมูลด้านความมั่นคง กอ.รมน. ในเอกสารฉบับนี้ มุ่งประเด็นไปที่ “ข้อมูลที่เกี่ยวข้องกับความมั่นคง” ซึ่งจำเป็นต้องมีระบบบริหาร รวมทั้งกระบวนการจัดการข้อมูลแต่ละประเภทในแต่ละขั้นตอนในห้วงเวลา บนวงจรชีวิตข้อมูล (Data Life Cycle) ในกรอบความรับผิดชอบของ กอ.รมน. ซึ่งได้แบ่งออกเป็น ๒ กลุ่ม เพื่อให้เกิดความชัดเจนในการดำเนินการ ประกอบด้วย วงจรชีวิตข้อมูลในกรอบงานรักษาความมั่นคงภายในราชอาณาจักร (ตามที่กฎหมายกำหนด) และวงจรชีวิตข้อมูลในกรอบงานศูนย์กลางข้อมูลด้านความมั่นคงตามรูปที่ ๓.๑ สรุปได้ดังนี้



รูปที่ ๓.๑ วงจรชีวิตข้อมูลในกรอบความรับผิดชอบของ กอ.รมน.

๓.๒.๑ วงจรชีวิตข้อมูลในกรอบงานรักษาความมั่นคงภายในราชอาณาจักร

กอ.รมน. เป็นส่วนราชการที่มีฐานะเป็นหน่วยงานของรัฐ ซึ่งมีหน้าที่ดำเนินการธรรมาภิบาลข้อมูลที่อยู่ในความรับผิดชอบ ตามประกาศคณะกรรมการพัฒนารัฐบาลดิจิทัล จึงกำหนดลำดับขั้นตอนวงจรชีวิตข้อมูลตามพันธกิจที่ได้รับมอบหมาย จำนวน ๕ ขั้นตอน (รูปที่ ๓.๑ วงจรชีวิตข้อมูล วงนอก) ดังนี้

๓.๒.๑.๑ ขั้นตอนสร้างและจัดเก็บ (Create and Store) : เนื่องจากขั้นตอนสร้างและขั้นตอนจัดเก็บ เป็นจุดเริ่มต้นของวงจรชีวิตข้อมูล ที่มีความเกี่ยวข้องสัมพันธ์ และทำงานร่วมกันอย่างใกล้ชิดต่อเนื่องกัน จึงกำหนดให้อยู่ในขั้นตอนเดียวกัน โดยมีรายละเอียด ดังนี้

๓.๒.๑.๑ (๑) ขั้นตอนการสร้าง : เป็นกระบวนการที่ทำให้เกิดข้อมูล ทั้งที่เป็นการดำเนินการด้วยบุคคล (Human) หรือด้วยเครื่องจักร (Machine) เช่น การสร้างข้อมูลด้วยเครื่องมืออิเล็กทรอนิกส์จากอุปกรณ์ตรวจจับสัญญาณ (Sensors) ฯลฯ

๓.๒.๑.๑ (๒) ขั้นตอนการจัดเก็บ : เป็นกระบวนการที่เกิดขึ้นต่อเนื่องจากกระบวนการสร้าง หรือการนำเข้าข้อมูลที่ได้จากการเชื่อมโยงแลกเปลี่ยนกับแหล่งข้อมูลที่อยู่ในกรอบอำนาจหน้าที่ของ กอ.รมน. โดยทำการบันทึกหรือนำข้อมูลเพื่อจัดเก็บลงแฟ้มข้อมูล (File) หรือระบบการจัดการฐานข้อมูล (Database Management System : DBMS) โดยมีขั้นตอนสำคัญที่ต้องพิจารณาดำเนินการ เพื่อให้ผู้ที่เกี่ยวข้องสามารถนำข้อมูลไปใช้งานในภายหลังได้โดยง่าย ปลอดภัย ไม่สูญหาย หรือถูกทำลาย ได้แก่ การแยกประเภท (Data Type) และจัดหมวดหมู่ข้อมูล (Data Category) เป็นต้น

๓.๒.๑.๒ ขั้นตอนใช้ (Use) : เป็นกระบวนการนำข้อมูลจากกระบวนสร้างและจัดเก็บเพื่อนำไปใช้ประโยชน์ตามพันธกิจของ กอ.รมน. ทั้งที่เป็นการใช้ประโยชน์จากข้อมูลโดยตรง และการใช้ประโยชน์ข้อมูลผ่านการวิเคราะห์ ประมวลผล เพื่อให้เกิดผลลัพธ์หรืออยู่ในรูปแบบการจัดทำรายงานที่เหมาะสมก่อน

๓.๒.๑.๓ ขั้นตอนเผยแพร่ (Publish) : เป็นกระบวนการนำเสนอ เผยแพร่ หรือเปิดเผยข้อมูลให้กับหน่วยงานของรัฐ หรือภาคเอกชน รวมถึงการเปิดเผยข้อมูลออกสู่สาธารณะภายใต้เงื่อนไขที่กำหนด

๓.๒.๑.๔ ขั้นตอนจัดเก็บถาวร (Archive) : เป็นกระบวนการคัดลอกหรือย้ายข้อมูลที่มีอายุเกินช่วงระยะเวลาใช้งาน และไม่มีการลบ ปรับปรุง แก้ไข หรือใช้งานอีกแล้ว ออกจากขั้นตอนการจัดเก็บปกติ โดยสามารถนำกลับมาใช้งานได้ใหม่เมื่อต้องการ

๓.๒.๑.๕ ขั้นตอนทำลาย (Destroy) : เป็นกระบวนการกำจัดข้อมูลที่ไม่ต้องการหรือครบระยะเวลาการจัดเก็บ ตามที่ระเบียบมาตรฐานที่กำหนด ทั้งนี้ข้อมูลที่ถูกทำลายแล้ว ต้องไม่สามารถนำกลับมาใช้งานได้อีก

๓.๒.๒ วงจรชีวิตข้อมูลในกรอบงานศูนย์กลางข้อมูลด้านความมั่นคง

ด้วยบทบาทศูนย์กลางข้อมูลด้านความมั่นคง ภายใต้แผนย่อยการพัฒนากลไกการบริหารจัดการความมั่นคงแบบองค์รวม แผนแม่บทภายใต้ยุทธศาสตร์ชาติประเด็นความมั่นคง กอ.รมน. จึงมีหน้าที่บูรณาการการเชื่อมโยงแลกเปลี่ยนข้อมูลกับหน่วยงานของรัฐและภาคเอกชน โดยจำเป็นต้องแบ่งแยกการบริหารและการจัดการข้อมูลออกจากวงจรชีวิตข้อมูลในกรอบงานปกติ เพื่อให้เป็นที่ยอมรับ ในเรื่องความโปร่งใส ชัดเจน และไม่มีการทับซ้อน โดยได้กำหนดลำดับขั้นตอนวงจรชีวิตข้อมูลในกรอบงานศูนย์กลางข้อมูลด้านความมั่นคง แบ่งเป็น ๕ ขั้น (รูปที่ ๓.๑ วงจรชีวิตข้อมูล วงใน) ดังนี้

๓.๒.๒.๑ ขั้นตอนบูรณาการ (Integrate)

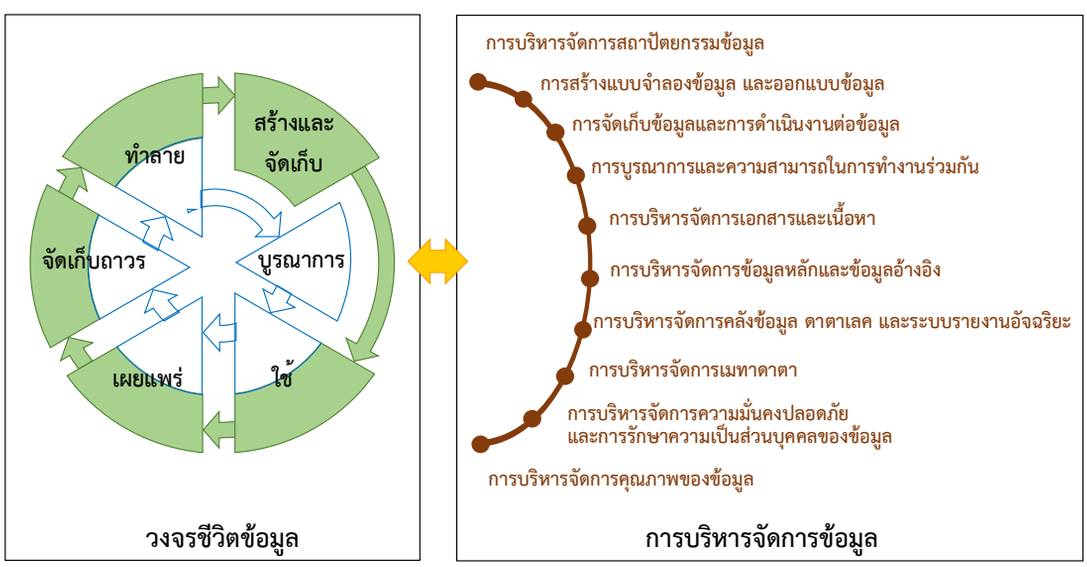
เป็นจุดเริ่มต้นของวงจรชีวิตข้อมูลในกรอบงานศูนย์กลางข้อมูลด้านความมั่นคง เพื่อให้ได้มาซึ่งข้อมูล ผ่านการเชื่อมโยงแลกเปลี่ยนกับหน่วยงานของรัฐหรือภาคเอกชน ซึ่งมีบทบาทเป็นเจ้าของข้อมูล โดยนำเข้าสู่ระบบจัดเก็บของศูนย์กลางข้อมูลด้านความมั่นคงอย่างเป็นหมวดหมู่ เพื่อให้ผู้ที่เกี่ยวข้องสามารถใช้งานได้โดยง่าย ปลอดภัย ไม่สูญหาย หรือถูกทำลายได้

๓.๒.๒.๒ ขั้นตอนอื่น ๆ

สำหรับขั้นตอนอื่น ๆ ในวงจรชีวิตข้อมูลในกรอบงานศูนย์กลางข้อมูลด้านความมั่นคงที่เหลือนั้น ประกอบด้วย ขั้นตอนใช้ ขั้นตอนเผยแพร่ ขั้นตอนจัดเก็บถาวร และขั้นตอนทำลาย มีหลักการทำงานในลักษณะเดียวกับขั้นตอนในวงจรชีวิตข้อมูลในกรอบความรับผิดชอบของ กอ.รมน. เพียงแต่เป็นการดำเนินการต่อข้อมูลในเชิงบูรณาการที่จำเป็นต้องดำเนินการในลักษณะแยกปฏิบัติ

๓.๓ การบริหารจัดการข้อมูล

เพื่อให้สามารถนำข้อมูลไปใช้งานได้อย่างมีประสิทธิภาพ ปลอดภัย และเชื่อถือได้ กอ.รมน. จำเป็นต้องกำหนดแนวทางการบริหารจัดการข้อมูล (Data Management) [๑๙] ในแต่ละขั้นตอนบนวงจรชีวิตข้อมูล อย่างเป็นระบบสอดคล้องกับมาตรฐานสากล จึงกำหนดองค์ประกอบในการบริหารจัดการข้อมูล รวม ๑๐ องค์ประกอบ (ตามรูปที่ ๓.๒) ดังนี้



รูปที่ ๓.๒ ความสัมพันธ์วงจรชีวิตข้อมูลและการบริหารจัดการ

๓.๓.๑ การบริหารจัดการสถาปัตยกรรมข้อมูล (Data Architecture Management)

เป็นกระบวนการจัดทำ ใช้ ทบทวน และปรับปรุงแบบจำลองสำหรับการอธิบายสถานภาพข้อมูลทั้งหมดของ กอ.รมน. อย่างเป็นภาพกว้าง โดยแสดงความสัมพันธ์และความเชื่อมโยงระหว่างกระบวนการทำงานกับข้อมูล ทั้งที่เป็นข้อมูลที่มีอยู่ในปัจจุบัน และข้อมูลที่ต้องการในอนาคต โดยสามารถนำไปใช้ในการสื่อสารทำความเข้าใจกับผู้ที่เกี่ยวข้อง เพื่อให้เกิดความเข้าใจและมองเห็นเป็นภาพเดียวกัน และเป็นจุดเริ่มต้นสำคัญที่ต้องดำเนินการควบคู่กับการจัดทำรายละเอียดขององค์ประกอบการบริหารจัดการข้อมูลด้านอื่น ๆ

๓.๓.๒ การสร้างแบบจำลองและออกแบบข้อมูล (Data Modeling and Design)

เป็นกระบวนการจัดทำแบบจำลองในรูปแบบไดอะแกรม เพื่อการออกแบบลักษณะโครงสร้างของข้อมูล แบ่งออกเป็น ๓ ขั้น ได้แก่ ขั้นออกแบบจำลองข้อมูลเชิงความคิด (Conceptual Data Model) ขั้นออกแบบจำลองข้อมูลเชิงตรรกะ (Logical Data Model) และขั้นออกแบบจำลองข้อมูลเชิงกายภาพ (Physical Data Model)

สำหรับการออกแบบจำลองข้อมูลเชิงความคิด ได้จากการรวบรวมและวิเคราะห์ความต้องการของผู้ใช้งาน เพื่อกำหนดเค้าโครงทางความคิดที่เชื่อมโยงความสัมพันธ์ของข้อมูลในขั้นต้น จากนั้นจึงเพิ่มรายละเอียด เช่น เขตข้อมูล (Data Field) ฯลฯ เพื่อจัดทำเป็นแบบจำลองข้อมูลเชิงตรรกะ นำไปสู่การจัดทำแบบจำลองข้อมูลเชิงกายภาพ ซึ่งเป็นแบบจำลองที่มีรายละเอียดครบถ้วนสมบูรณ์ (เช่น รูปแบบและขนาดของข้อมูล ฯลฯ) และพร้อมนำไปใช้งานจริง

๓.๓.๓ การจัดเก็บและการดำเนินงานต่อข้อมูล (Data Storage and Operations)

การจัดเก็บและการดำเนินงานต่อข้อมูล เป็นกระบวนการเกี่ยวกับการวางแผน จัดเก็บ ใช้ สำรองและกู้คืน จัดเก็บถาวร และกระบวนอื่นๆ ที่เกี่ยวข้องกับข้อมูลที่เป็นแบบมีโครงสร้าง (Structured Data) รวมถึงการปรับปรุงประสิทธิภาพ คุณภาพ และรักษาความมั่นคงปลอดภัยของฐานข้อมูล ให้พร้อมใช้งานได้ตลอดวงจรชีวิตของข้อมูล

๓.๓.๔ การบูรณาการและความสามารถในการทำงานร่วมกัน (Data Integration and Interoperability)

การบูรณาการข้อมูล (Data Integration) เป็นกระบวนการที่มุ่งเน้นการแปลงข้อมูล (Data Transform) หรือแลกเปลี่ยน โอนย้ายข้อมูลมาจากแหล่งข้อมูลต่าง ๆ ของหน่วยงานของรัฐหรือของภาคเอกชน โดยหาความสัมพันธ์ ความเกี่ยวข้อง หรือความสอดคล้องของข้อมูล แล้วเชื่อมโยงผ่านข้อมูลหลัก (Master Data) เพื่อรวบรวม จัดเก็บเข้าไปอยู่ในแหล่งข้อมูลเดียวกัน เช่น คลังข้อมูล (Data Warehouse) หรือ ดาตาเลค (Data Lake) ฯลฯ ทั้งนี้ เพื่อให้เกิดการบูรณาการและใช้งานข้อมูลดังกล่าวร่วมกัน (Interoperability) อย่างมีประสิทธิภาพ จึงกำหนดให้จัดทำมาตรฐานหรือข้อตกลงในการใช้คุณลักษณะเพื่อการแลกเปลี่ยนหรือสื่อสารข้อมูลระหว่างหน่วยงานหรือระบบงาน ให้มีความชัดเจน เช่น การแลกเปลี่ยนข้อมูลในรูปแบบส่วนต่อประสานโปรแกรมประยุกต์ หรือเอพีไอ (API : Application Programming Interfaces) ซึ่งมีขีดความสามารถในการควบคุมและจัดการคุณภาพของข้อมูลที่รวบรวมจากแหล่งต่าง ๆ ได้แบบอัตโนมัติ เป็นต้น

๓.๓.๕ การบริหารจัดการเอกสารและเนื้อหา (Document and Content Management)

เป็นกระบวนการวางแผนการจัดการ จัดเก็บ เข้าถึง ใช้ และควบคุมกิจกรรมต่าง ๆ ที่เกี่ยวกับข้อมูลที่เป็นแบบกึ่งโครงสร้าง (Semi-Structured Data) หรือแบบไม่มีโครงสร้าง (Unstructured Data) เช่น ข้อมูลที่เก็บอยู่ในรูปแบบกระดาษ และไฟล์อิเล็กทรอนิกส์ที่เป็นข้อความ รูปภาพ เสียง ภาพเคลื่อนไหว ฯลฯ โดยมุ่งเน้นในเรื่องการบริหารจัดการเพื่อให้สามารถเข้าถึง รวมทั้งรักษาความถูกต้อง ความสมบูรณ์ของข้อมูลได้อย่างมีประสิทธิภาพ

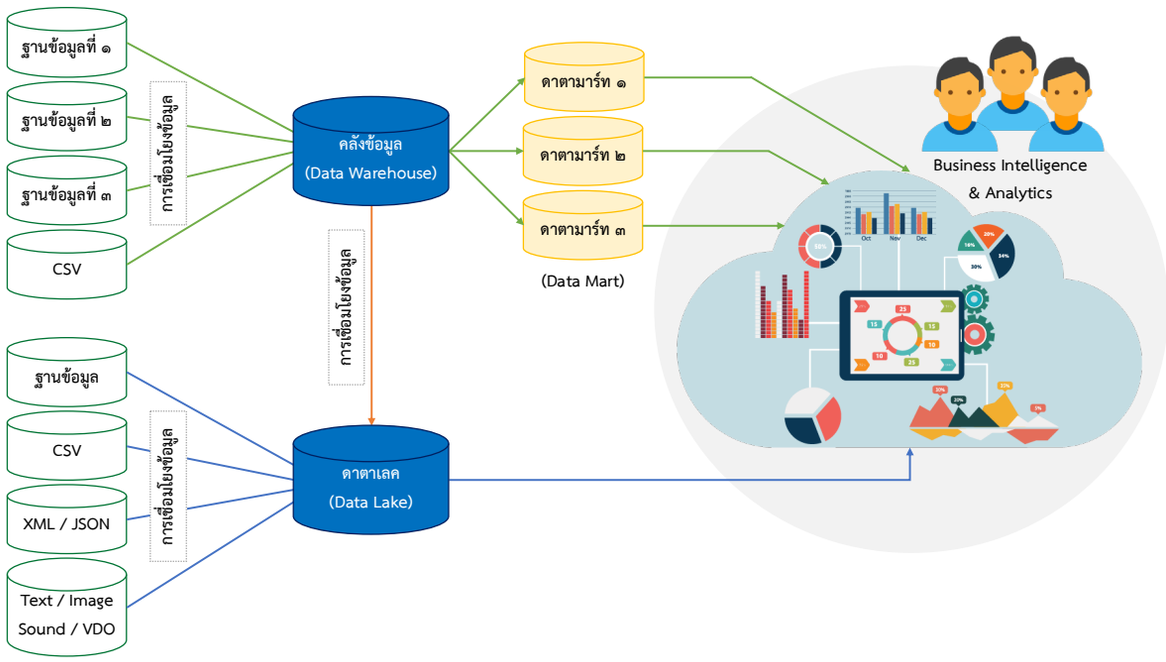
๓.๓.๖ การบริหารจัดการข้อมูลหลักและข้อมูลอ้างอิง (Master and Reference Data Management)

เป็นกระบวนการเกี่ยวกับการบริหารจัดการข้อมูลที่ได้บูรณาการเข้ามาจัดเก็บไว้ในแหล่งข้อมูลเดียวกัน โดยหน่วยงานและผู้ที่มีส่วนเกี่ยวข้อง สามารถเข้าถึงและใช้งานข้อมูลร่วมกันได้อย่างมีประสิทธิภาพ ลดความซ้ำซ้อน ฯลฯ ด้วยการกำหนดและปรับปรุงมาตรฐานข้อมูล ให้มีข้อมูลหลัก (Master Data) และข้อมูลอ้างอิง (Reference Data) โดยข้อมูลอ้างอิง จะเป็นข้อมูลที่มีการใช้งานและเป็นที่รู้จักกันอย่างเป็นวงกว้าง และมีความเป็นสากล มีโอกาสเปลี่ยนแปลงค่อนข้างน้อย ได้แก่ รหัสไปรษณีย์ หน่วยวัดระยะทาง ฯลฯ ขณะที่ข้อมูลหลัก เป็นข้อมูลที่มีการใช้งานในวงจำกัด เช่น ข้อมูลบุคลากรหรือข้อมูลครุภัณฑ์ ภายในหน่วยงาน ฯลฯ ซึ่งมีโอกาสหรือความถี่ในการเปลี่ยนแปลงรายละเอียดข้อมูล ค่อนข้างมาก

๓.๓.๗ การบริหารจัดการคลังข้อมูล ดาตาเลค และระบบรายงานอัจฉริยะ (Data Warehousing, Data Lake and Business Intelligence Management)

เป็นการดำเนินการเกี่ยวกับการบูรณาการเชื่อมโยงข้อมูลจากแหล่งข้อมูลของหน่วยงานของรัฐและภาคเอกชน โดยนำเข้ามาจัดเก็บและเตรียมการให้มีความพร้อมในการใช้สนับสนุนการจัดทำรูปแบบรายงานอัจฉริยะ (Business Intelligences) และการวิเคราะห์ประมวลผลข้อมูล (Data Analytics) แบ่งเป็น ๒ ประเภท ตามรูปที่ ๓.๓ ดังนี้

๓.๓.๗.๑ “คลังข้อมูล (Data Warehouse)” ใช้สำหรับจัดเก็บข้อมูลที่มีโครงสร้างข้อมูลและนำเข้าโดยใช้วิธี “ETL (Extract-Transform-Load)” ซึ่งเป็นกระบวนการ “ดึง-แปลง-นำเข้า” ข้อมูลจากแหล่งของข้อมูลภายนอก แล้วปรับรูปแบบ รวมทั้งจัดเป็นกลุ่มข้อมูลย่อยในรูปแบบดาตามาร์ท (Data Mart) ที่ตรงกับความต้องการของแต่ละกลุ่มผู้ใช้งานข้อมูล



รูปที่ ๓.๓ การบริหารจัดการคลังข้อมูลและดาตาเลค

๓.๓.๗.๒ “ดาตาเลค (Data Lake)” ใช้สำหรับรวบรวมข้อมูลหลากหลายรูปแบบ ทั้งที่เป็นข้อมูลแบบมีโครงสร้าง ข้อมูลกึ่งโครงสร้าง และข้อมูลที่ไม่มีโครงสร้าง โดยข้อมูลถูกจัดเก็บไว้ในรูปแบบที่เหมือนหรือใกล้เคียงกับรูปแบบที่ได้รับมาจากแหล่งข้อมูลต้นฉบับ ทั้งนี้ สามารถใช้ประโยชน์จากดาตาเลค เป็นพื้นที่สำรองข้อมูลได้อีกด้วย

๓.๓.๘ การบริหารจัดการเมทาดาตา (Metadata Management)

เป็นกระบวนการวางแผน กำหนดมาตรฐาน ดำเนินการ และการควบคุม “คำอธิบายข้อมูล” หรือ “เมทาดาตา” ของแต่ละชุดข้อมูล ซึ่งช่วยให้เกิดความเข้าใจในรายละเอียดเกี่ยวกับชุดข้อมูล รวมถึงวัตถุประสงค์การนำข้อมูลไปใช้ ระบบและขั้นตอนการดำเนินการที่เกี่ยวข้อง เป็นต้น ทั้งนี้ เพื่อให้ได้เมทาดาตาที่มีคุณภาพ และสามารถนำไปใช้งานร่วมกับเมทาดาตาอื่น ๆ ได้

๓.๓.๙ การบริหารจัดการความมั่นคงปลอดภัยและการรักษาความเป็นส่วนบุคคลของข้อมูล (Data Security and Privacy Management)

เป็นกระบวนการวางแผน พัฒนา และดำเนินการตามนโยบาย กฎหมาย และแนวปฏิบัติด้านการป้องกันรักษาความมั่นคงปลอดภัยข้อมูลและการรักษาความเป็นส่วนบุคคลของข้อมูล (ตามรูปที่ ๓.๔) อย่างเป็นระบบ ดังนี้

รูปที่ ๓.๔ ความสัมพันธ์ระหว่างการป้องกันและการรักษาความมั่นคงปลอดภัยข้อมูล

๓.๓.๙.๑ การป้องกันความปลอดภัยข้อมูล ได้แก่ การรักษาชั้นความลับ (Confidentiality) ความถูกต้องของข้อมูล (Integrity) และความพร้อมใช้งานของข้อมูล (Availability)

๓.๓.๙.๒ การรักษาความปลอดภัยของข้อมูล ได้แก่ การพิสูจน์ตัวตน (Authentication) การกำหนดสิทธิ์ (Authorization) และการเข้าถึง (Access)

๓.๓.๙.๓ การรักษาความเป็นส่วนบุคคลของข้อมูล เป็นกิจกรรมที่ต้องให้ความระมัดระวังในทุกขั้นตอน ตั้งแต่การรวบรวมข้อมูลจากเจ้าของข้อมูลส่วนบุคคล การจัดเก็บ การใช้ การเผยแพร่ การนำเสนอข้อมูลที่ต้องเป็นไปตามวัตถุประสงค์ของการรวบรวมข้อมูลและได้รับความยินยอมจากเจ้าของข้อมูลเป็นรายบุคคล หรือเป็นไปตามขอบเขตหน้าที่และอำนาจที่กฎหมายกำหนดไว้ เท่านั้น

๓.๓.๑๐ การบริหารจัดการคุณภาพของข้อมูล (Data Quality Management)

เป็นกระบวนการวางแผน ดำเนินการ ปรับปรุง และควบคุมคุณภาพของข้อมูลในวงจรชีวิตข้อมูล ให้มีความถูกต้อง (Accuracy) ครบถ้วน (Completeness) สอดคล้องกัน (Consistency) เป็นปัจจุบัน (Timeliness) ตรงตามความต้องการของผู้ใช้ (Relevancy) และพร้อมใช้งาน (Availability) ตามรูปที่ ๓.๕ โดยให้มีการวัดระดับคุณภาพของข้อมูลและประสิทธิภาพของการนำข้อมูลไปใช้ อย่างต่อเนื่อง

รูปที่ ๓.๕ มิติของคุณภาพข้อมูล

๓.๔ ขอบเขตงานบูรณาการข้อมูล

ในข้อ ๓.๔ นี้ เป็นการสรุปขอบเขตงานพื้นฐานที่เกี่ยวกับการธรรมาภิบาลข้อมูลของ กอ.รมน. ซึ่งยึดกรอบแนวคิดในการกำหนดกระบวนการธรรมาภิบาลข้อมูลภาครัฐ [๑๐] ครอบคลุมงานทั้งในมิติการวางแผนและกำหนดทิศทางการดำเนินงานในภาพรวมของระดับบริหาร (Management Level) และการดำเนินงานในระดับปฏิบัติ (Operation Level) แบ่งออกเป็น ๔ กลุ่มงาน ตามรูปที่ ๓.๖ ประกอบด้วย (๑) การเลือกข้อมูลเพื่อดำเนินการธรรมาภิบาล (๒) การระบุเป้าหมายในการธรรมาภิบาล (๓) การกำหนดมาตรฐานและแนวปฏิบัติ และ (๔) การบริหารจัดการบุคลากร

๓.๔.๑ การเลือกข้อมูลเพื่อดำเนินการธรรมาภิบาล

“การวางแผนเลือกข้อมูล” ที่จะนำเข้ามาบูรณาการและรวมกันให้เป็นข้อมูลขนาดใหญ่อย่างเป็นระบบ นับว่าเป็นจุดเริ่มต้นงานธรรมาภิบาลข้อมูลที่สำคัญ โดยใช้วิธีการศึกษา สำรวจข้อมูลจากภูมิทัศน์ข้อมูล (Data Landscape) ซึ่งเป็นแหล่งข้อมูลของหน่วยงานของรัฐและภาคเอกชน ที่มีความเกี่ยวข้องทุกระบบแล้วทำการตรวจสอบวิเคราะห์ความต้องการใช้งานข้อมูลในแต่ละประเภท (เช่น ข้อมูลสาธารณะ ข้อมูลส่วนบุคคล ข้อมูลความมั่นคง และข้อมูลที่ระดับชั้นความลับ ฯลฯ) ให้มีความชัดเจน ก่อนการเลือกข้อมูลเพื่อนำมาใช้ประโยชน์สนับสนุนการปฏิบัติงานตามพันธกิจของ กอ.รมน. หรือภาระงานศูนย์กลางข้อมูลด้านความมั่นคง ต่อไป

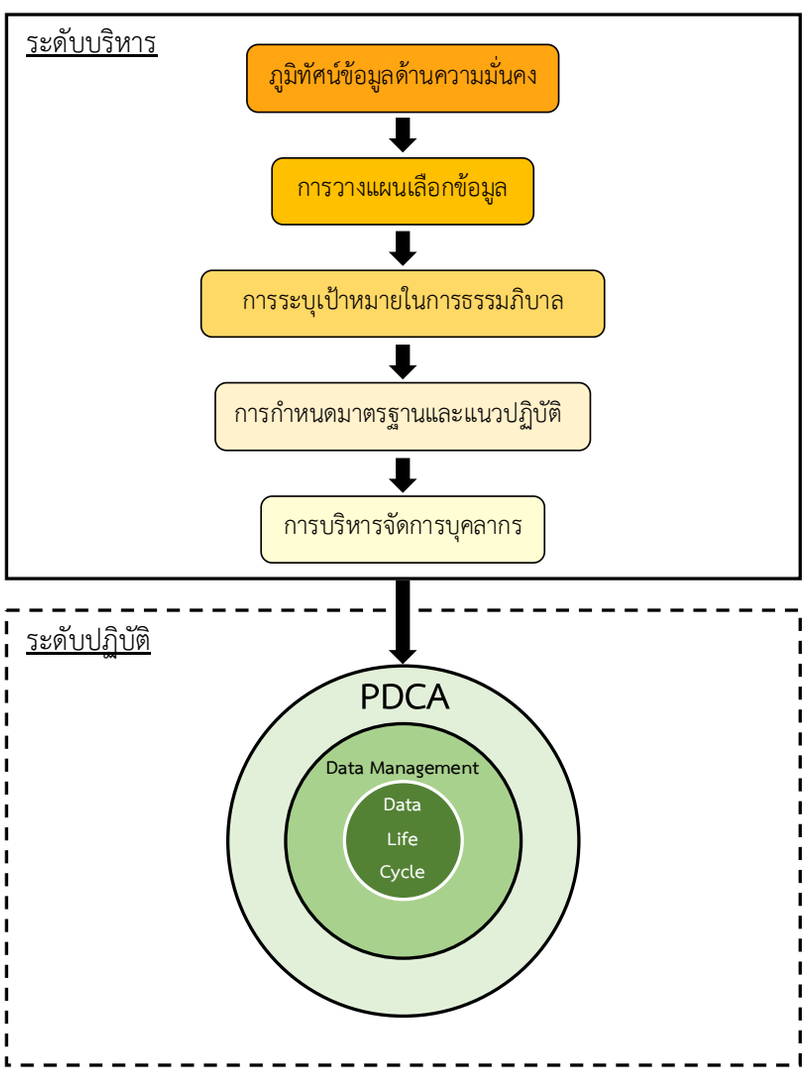
๓.๔.๒ การระบุเป้าหมายในการธรรมาภิบาล

ภายหลังการเลือกข้อมูลที่จะดำเนินการธรรมาภิบาลข้อมูลครบแล้ว เพื่อให้ผู้เกี่ยวข้องมีรายละเอียดเกี่ยวกับความต้องการดำเนินการต่อข้อมูลที่เป็นรูปธรรม จำเป็นต้องระบุเป้าหมายในการธรรมาภิบาลข้อมูลให้มีความชัดเจน ดังนี้

๓.๔.๒.๑ เป้าหมายด้านคุณภาพข้อมูล : ประกอบด้วย ระดับของความถูกต้อง (Accuracy) ความครบถ้วน (Completeness) ความสอดคล้อง/ความต้องกัน (Consistency) ความเป็นปัจจุบัน (Timeliness) ความตรงตามความต้องการใช้งาน (Relevancy) และความพร้อมใช้งาน (Availability) ของข้อมูล ฯลฯ

๓.๔.๒.๒ เป้าหมายด้านการป้องกันและรักษาความมั่นคงปลอดภัยข้อมูล : ประกอบด้วย ระดับของการรักษาชั้นความลับ ความถูกต้องของข้อมูล ความพร้อมใช้งาน และความเป็นส่วนบุคคลของข้อมูล ฯลฯ

๓.๔.๒.๓ เป้าหมายอื่น ๆ : ได้แก่ ระดับประสิทธิภาพการดำเนินการ ผลกระทบจากการดำเนินการ วิธีการจัดการข้อมูล และความคุ้มค่า ฯลฯ



รูปที่ ๓.๖ ขอบเขตงานพื้นฐานทั่วไปของการบูรณาการข้อมูล

๓.๔.๓ การกำหนดมาตรฐานและแนวปฏิบัติ

ผลผลิตที่ได้จากการดำเนินกลุ่มงานในข้อ ๓.๔.๑ - ๓.๔.๒ คือการรวบรวมความต้องการเบื้องต้นเกี่ยวกับข้อมูลที่เป็นเป้าหมายในการบูรณาการฯ (Initial Requirements of Data) ซึ่งหากนำมาจัดหมวดหมู่ และปรับรูปแบบเพื่อกำหนดเป็นมาตรฐานกลาง (Standardization) รวมทั้งกำหนดนโยบายซึ่งกลไกการบริหารจัดการข้อมูลดังกล่าวในเชิงกลยุทธ์ (Strategic Data Management) และการกำหนดแนวปฏิบัติ (Operation Procedures) ให้มีความชัดเจน โดยครอบคลุมงานตั้งแต่การวางแผน ดำเนินการ ตรวจสอบ กำกับดูแล และประเมินผลในแต่ละขั้นตอนบนวงจรชีวิตข้อมูล ก็จะทำให้กรอบการธรรมาภิบาลข้อมูลของ กอ.รมน. มีองค์ประกอบที่ครบถ้วน สมบูรณ์

๓.๔.๔ การบริหารจัดการบุคลากร

กลุ่มงานสุดท้าย เป็นกิจกรรมที่มีความสำคัญสูงสุด คือการนำนโยบายการบริหารจัดการ มาตรฐาน และแนวปฏิบัติ ไปสู่การปฏิบัติจริงให้เกิดผลสัมฤทธิ์ตามพันธกิจของ กอ.รมน. และศูนย์กลางข้อมูลด้านความมั่นคง ผ่านการบริหารจัดการด้านบุคลากรที่เกี่ยวกับการธรรมาภิบาลข้อมูล เช่น การจัดโครงสร้างบุคลากร การมอบหมายหน้าที่และอำนาจ การฝึกอบรม เสริมสร้างความตระหนักรู้ การกำหนดช่องทางการติดต่อสื่อสาร การเสริมสร้างความสัมพันธ์ระหว่างผู้ปฏิบัติงาน อันนำไปสู่การสร้างวัฒนธรรมองค์กรอย่างมีธรรมาภิบาลที่มั่นคงยั่งยืน

๓.๕ กระบวนการธรรมาภิบาลข้อมูล

ปัจจัยสำคัญที่ทำให้การดำเนินงานไม่ว่าเป็นเรื่องใด สามารถบรรลุเป้าหมายได้ คือการนำหลักแนวคิดหรือนโยบายไปสู่การปฏิบัติจริง ได้อย่างเป็นระบบและต่อเนื่อง ซึ่งธรรมาภิบาลข้อมูลด้านความมั่นคงฉบับนี้ ได้นำหลักการปฏิบัติงานของวงจรเดมมิ่ง (Deming Cycle) หรือวงล้อพีดีซีเอ (PDCA Cycle) [๒๐] มาประยุกต์ใช้ในการกำหนดกระบวนการธรรมาภิบาลข้อมูล โดยมีวงรอบการดำเนินการ เริ่มจากวางแผน ดำเนินการ ตรวจสอบ และปรับปรุงแก้ไข เพื่อให้บรรลุเป้าหมายที่กำหนด ทั้งในด้านประสิทธิภาพ คุณภาพ ความน่าเชื่อถือ ความสอดคล้องกับระเบียบกฎหมายหรือนโยบายที่เกี่ยวข้อง ฯลฯ อย่างเป็นวงรอบต่อเนื่อง ตามรูปที่ ๓.๗ ดังนี้

๓.๕.๑ วางแผน (Plan)

จุดเริ่มต้นของการนำวงจรเดมมิ่งมาใช้สนับสนุนการธรรมาภิบาลข้อมูลของ กอ.รมน. คือ การวางแผนปฏิบัติงาน (Action Plan) ภายใต้กรอบนโยบายและแนวปฏิบัติที่กำหนดในธรรมาภิบาลข้อมูลด้านความมั่นคง กอ.รมน. ฉบับนี้ โดยมีเป้าหมายขับเคลื่อนการบูรณาการและใช้งานข้อมูลเพื่อเปลี่ยนผ่านประเทศและ กอ.รมน. ไปสู่องค์กรที่ขับเคลื่อนด้วยข้อมูล (Data Driven Organization) เพื่อความมั่นคงและผลประโยชน์แห่งชาติ ทั้งนี้ การวางแผนปฏิบัติงานที่ดี จำเป็นต้องกำหนดรายละเอียดทั้งในด้านประเด็นเป้าหมาย ขอบเขตงาน วิธีการ กรอบระยะเวลา ผู้รับผิดชอบ ผู้ที่มีส่วนเกี่ยวข้อง งบประมาณ และเครื่องมือสนับสนุนการดำเนินงาน ฯลฯ ให้มีความชัดเจน ก่อนนำไปประกาศเพื่อให้ผู้เกี่ยวข้อง ทราบหรือนำไปใช้ปฏิบัติต่อไป

รูปที่ ๓.๗ วงรอบงานธรรมาภิบาลข้อมูลระดับปฏิบัติ

๓.๕.๒ ดำเนินการ (Do)

กระบวนการธรรมาภิบาลข้อมูลในขั้นต่อจากการวางแผน คือขั้นดำเนินการตามแผนปฏิบัติงานในข้อ ๓.๕.๑ โดยส่วนงานและบุคลากรที่มีส่วนเกี่ยวข้อง ซึ่งการดำเนินการต้องมีความสอดคล้อง ไม่ขัดต่อระเบียบ กฎหมาย นโยบาย มาตรฐาน และแนวปฏิบัติที่กำหนด และต้องรายงานความคืบหน้าผลการปฏิบัติงาน รวมทั้งประเด็นปัญหาข้อขัดข้องที่ตรวจพบระหว่างปฏิบัติงาน ให้ผู้บังคับบัญชาตามลำดับชั้น หรือผู้ที่มีความเกี่ยวข้องทราบ (ถ้าจำเป็น) ทั้งนี้ กอ.รมน. ต้องจัดตั้งทีมปรึกษา ให้ความรู้ คำแนะนำ รวมทั้งให้การสนับสนุนการธรรมาภิบาลข้อมูลแก่ส่วนงานต่าง ๆ ของ กอ.รมน. ด้วย

๓.๕.๓ ตรวจสอบ (Check)

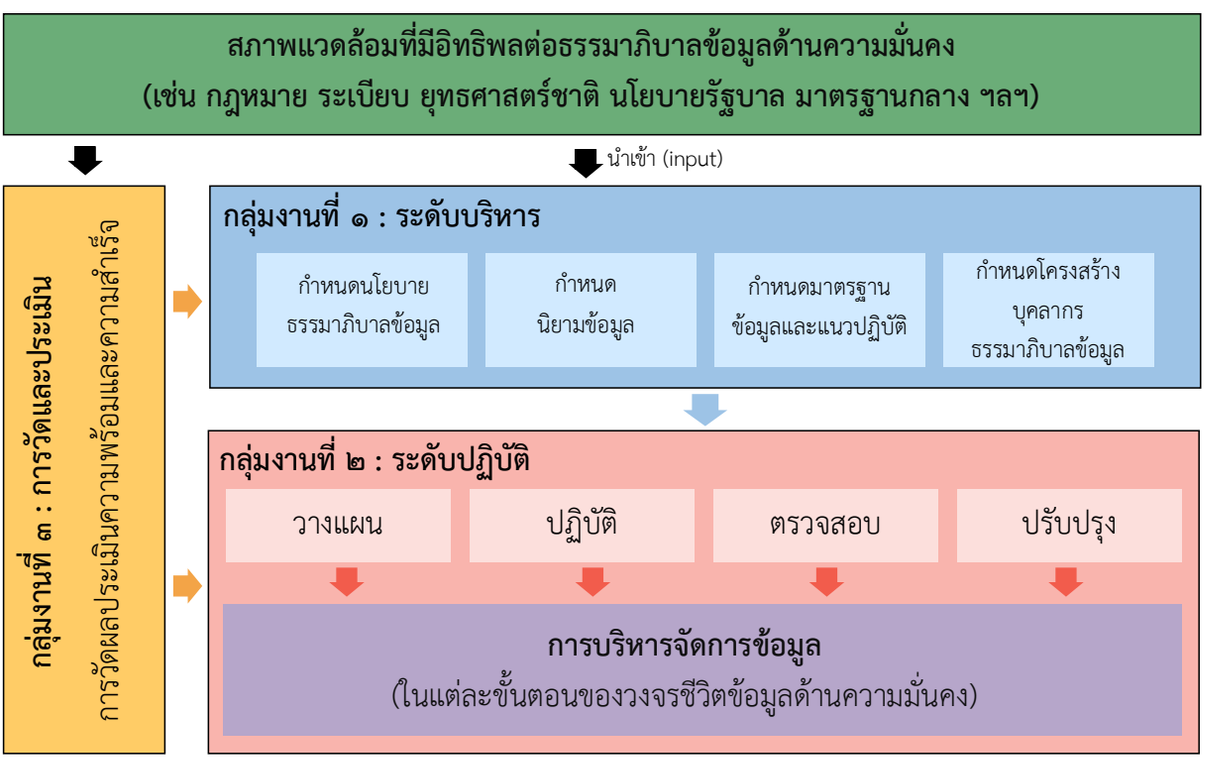
กระบวนการธรรมาภิบาลข้อมูลในขั้นตอนที่ ๓ คือขั้นตรวจสอบ ซึ่งรวมถึงงานวัดผลการดำเนินการในข้อ ๓.๕.๒ เปรียบเทียบกับเป้าหมายและแผนปฏิบัติงานในข้อ ๓.๕.๑ แล้วจัดทำเป็นรายงานให้ผู้บังคับบัญชาตามลำดับชั้น หรือผู้ที่มีความเกี่ยวข้อง ทราบด้วย (หากจำเป็น) ทั้งนี้ กอ.รมน. และส่วนงานขึ้นตรงของ กอ.รมน. ที่เป็นเจ้าของข้อมูล จำเป็นต้องแต่งตั้งผู้รับผิดชอบ เพื่อมอบหมายหน้าที่ในการตรวจสอบ วัดผล และจัดทำรายงาน ให้มีความชัดเจนด้วย

๓.๕.๔ ปรับปรุงแก้ไข (Act)

กระบวนการธรรมาภิบาลข้อมูลในขั้นตอนสุดท้ายของวงจรเดมมิ่ง คือขั้นปรับปรุงแก้ไข โดยบุคลากรที่เกี่ยวข้อง ต้องนำผลการตรวจสอบจากรายงานในข้อ ๓.๕.๓ มาทบทวน วิเคราะห์ปัญหา สาเหตุ รวมทั้งเสนอแนะหัวข้อการปรับปรุงแก้ไข เพื่อนำไปใช้ในการปรับปรุงแผนปฏิบัติการ อย่างเป็นวงรอบต่อเนื่อง (Continual Improvement)

ในบทที่ ๓ ได้สรุปหลักการที่นำมาใช้ประกอบการจัดทำธรรมาภิบาลข้อมูลด้านความมั่นคงของ กอ.รมน. เริ่มจากการกำหนดกรอบวงจรชีวิตข้อมูลที่ต้องแบ่งการควบคุม ออกเป็น ๒ กลุ่ม ทั้งวงจรชีวิตข้อมูลที่อยู่ในความรับผิดชอบของ กอ.รมน. เอง และวงจรชีวิตข้อมูลที่ได้บูรณาการเชื่อมโยงมาจากหน่วยงานภายนอก และเมื่อนำวงจรชีวิตข้อมูลมาประยุกต์ใช้กับหลักการบริหารจัดการข้อมูล ผสมผสานกับการกำหนดขอบเขตงานที่เป็นไปตามกรอบธรรมาภิบาลข้อมูลภาครัฐ และนำทฤษฎีวงจรเดมมิ่งมาใช้ออกแบบการขับเคลื่อนการดำเนินงานในลักษณะเป็นวงรอบต่อเนื่อง จึงทำให้ภาพของการทำงานธรรมาภิบาลข้อมูลของ กอ.รมน. มีความชัดเจนและเป็นรูปธรรม ยิ่งขึ้น

ในรูปที่ ๓.๘ เป็นผังแสดงความสัมพันธ์เชื่อมโยงองค์ประกอบที่มีอิทธิพลต่อการกำหนดกรอบการธรรมาภิบาลข้อมูลของ กอ.รมน. แบบองค์รวม ทั้งในบริบทสภาพแวดล้อมภายนอกที่กล่าวในบทที่ ๒ และหลักการที่ใช้กำหนดกระบวนการธรรมาภิบาลข้อมูลในบทที่ ๓ โดยแบ่งงานออกเป็น ๓ กลุ่ม ประกอบด้วยกลุ่มงานระดับบริหาร (เชิงนโยบาย) กลุ่มงานระดับปฏิบัติ และกลุ่มงานวัดและประเมินผลการปฏิบัติ ซึ่งจะกล่าวในรายละเอียดในบทต่อ ๆ ไป

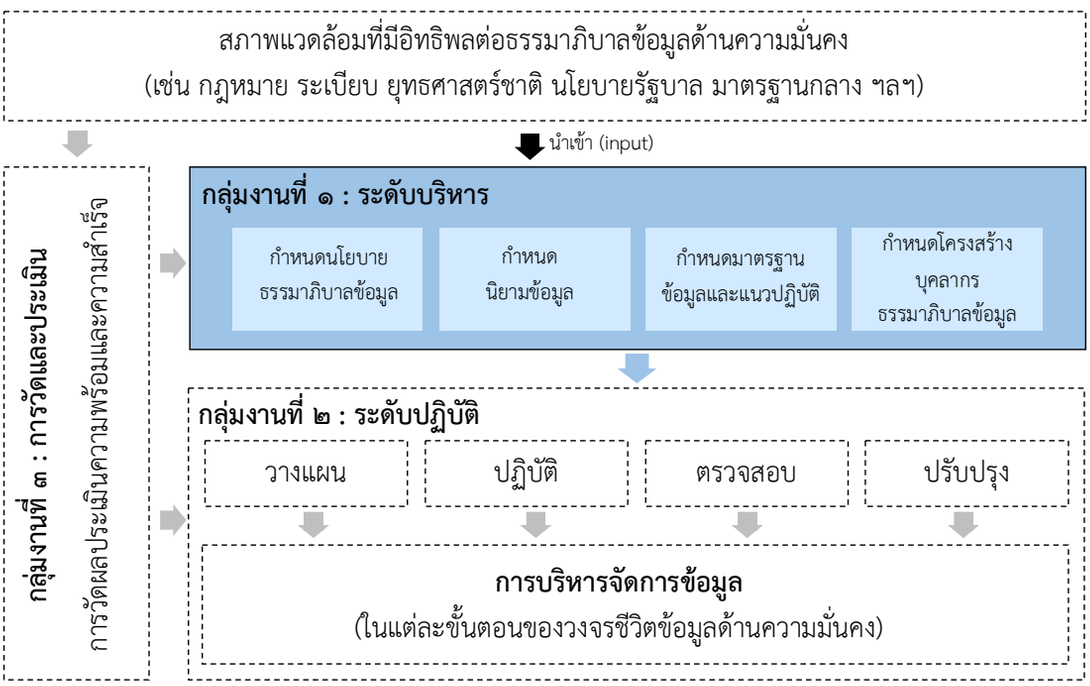


รูปที่ ๓.๘ ผังแสดงความสัมพันธ์เชื่อมโยงองค์ประกอบที่มีอิทธิพลต่อการธรรมาภิบาลข้อมูลของ กอ.รมน.

บทที่ ๔
การธรรมาภิบาลข้อมูลในภาพรวมของ กอ.รมน.

๔.๑ กล่าวนำ

ในบทที่ ๔ เป็นการลงในรายละเอียดขององค์ประกอบการธรรมาภิบาลข้อมูลระดับบริหารของ กอ.รมน. ซึ่งเป็นกลไกหลักในการขับเคลื่อนงานในภาพรวม ตั้งแต่การกำหนดวิสัยทัศน์ และเป้าหมายในการดำเนินงาน การกำหนดกรอบนโยบาย การกำหนดขอบเขตงานผ่านการนิยามข้อมูล การวางกรอบมาตรฐานและแนวปฏิบัติ รวมทั้ง โครงสร้างและความรับผิดชอบของบุคคลากร ผู้มีส่วนได้ส่วนเสียที่เกี่ยวข้องกับการธรรมาภิบาลข้อมูลทั้งหมด รายละเอียดตามรูปที่ ๔.๑



รูปที่ ๔.๑ การธรรมาภิบาลข้อมูลในภาพรวม (ระดับบริหาร) ของ กอ.รมน.

๔.๒ วิสัยทัศน์และพันธกิจ กอ.รมน.

กอ.รมน. ได้จัดทำเอกสารธรรมาภิบาลข้อมูล เพื่อใช้เป็นเครื่องมือสนับสนุนการเปลี่ยนผ่านไปสู่องค์กรที่ขับเคลื่อนด้วยข้อมูล (Data Driven Organization) ภายใต้แผนปฏิบัติราชการประจำปี [๒๑] โดยมีเป้าหมายให้ “ประเทศชาติมั่นคง ประชาชนมีความสุข” สอดคล้องเชื่อมโยงกับยุทธศาสตร์ชาติด้านความมั่นคง โดยกำหนดวิสัยทัศน์ พันธกิจ และวิสัยทัศน์ธรรมาภิบาลข้อมูลของ กอ.รมน. ไว้ดังนี้

๔.๒.๑ วิสัยทัศน์ของ กอ.รมน.

“กอ.รมน. เป็นองค์กรหลักในการบูรณาการ อำนวยการ และประสานการปฏิบัติในการรักษาความมั่นคงภายในราชอาณาจักร เพื่อให้เกิดความมั่นคงของรัฐและความสงบสุขของประชาชน”

๔.๒.๒ พันธกิจของ กอ.รมน.

๔.๒.๒.๑ ติดตาม แจ้งเตือน และประเมินแนวโน้มของสถานการณ์ภัยคุกคามความมั่นคงทั้งภายในและภายนอกราชอาณาจักร

๔.๒.๒.๒ บูรณาการแนวทาง และแผนงานในการป้องกันและแก้ไขปัญหาที่มีผลกระทบต่อความมั่นคง

๔.๒.๒.๓ อำนวยการ ประสานงาน และเสริมการปฏิบัติป้องกันและแก้ไขปัญหาที่มีผลกระทบต่อความมั่นคงตามแผนปฏิบัติการ แผนงาน โครงการ หรือการปฏิบัติงาน เป็นไปตามแผนหรือเป้าหมายที่วางไว้และเป็นไปอย่างมีประสิทธิภาพ

๔.๒.๒.๔ ติดตามและประเมินผลการดำเนินการแก้ไขปัญหาที่มีผลกระทบต่อความมั่นคงตามแผนปฏิบัติการ และแผนงานโครงการที่รองรับแผนแม่บทประเด็นความมั่นคงและแผนระดับที่ ๒ อื่น ๆ

๔.๒.๒.๕ ส่งเสริมให้ทุกภาคส่วนเข้ามามีส่วนร่วมในการป้องกันและแก้ไขปัญหาที่มีผลกระทบต่อความมั่นคง

๔.๒.๒.๖ สร้างความตระหนักรู้แก่ประชาชนถึงหน้าที่ที่ต้องพิทักษ์รักษาไว้ซึ่งชาติ ศาสนา และพระมหากษัตริย์ และเพื่อสร้างความสามัคคีของคนในชาติ

๔.๒.๓ วิสัยทัศน์ธรรมาภิบาลข้อมูลของ กอ.รมน.

“กอ.รมน. เป็นองค์กรหลักในการบูรณาการข้อมูลเพื่อใช้สนับสนุนพันธกิจให้เกิดความมั่นคงของรัฐและความสงบสุขของประชาชน โดยมีระบบบริหารจัดการข้อมูลที่ดี มีคุณภาพ ปลอดภัย โปร่งใส และตรวจสอบได้”

๔.๓ นโยบายธรรมาภิบาลข้อมูล

เป้าหมายของการเชื่อมโยงแลกเปลี่ยนข้อมูลจากแหล่งข้อมูลต่าง ๆ เพื่อบูรณาการให้เป็นข้อมูลขนาดใหญ่ (Big Data) อันเป็นสิ่งจำเป็นยิ่งต่อการบริหารราชการแผ่นดินในปัจจุบัน โดย กอ.รมน. ให้ความสำคัญและมีความมุ่งมั่นในการขับเคลื่อนการดำเนินการ รวมทั้งจัดทำธรรมาภิบาลข้อมูลฉบับนี้ขึ้น เพื่อให้การบริหารจัดการข้อมูลทั้งที่อยู่ในความครอบครองหรืออยู่ในความรับผิดชอบของ กอ.รมน. โดยตรง และข้อมูลในบทบาทศูนย์กลางข้อมูลด้านความมั่นคง สามารถปฏิบัติได้จริง มีประสิทธิภาพ โปร่งใส และเชื่อถือได้ ภายในปีงบประมาณ พ.ศ. ๒๕๖๕ จึงกำหนดนโยบายธรรมาภิบาลข้อมูลของ กอ.รมน. แบ่งเป็น ๓ ด้าน ดังนี้

๔.๓.๑ นโยบายขับเคลื่อนธรรมาภิบาลข้อมูลของส่วนงานใน กอ.รมน.

๔.๓.๑.๑ ส่งเสริมการพัฒนา กำกับดูแล ตรวจสอบ และประเมินผลการขับเคลื่อนธรรมาภิบาลข้อมูลภายใน กอ.รมน. ให้เป็นไปตามกรอบแนวทางธรรมาภิบาลข้อมูลภาครัฐ กฎหมาย และระเบียบที่เกี่ยวข้อง เพื่อเสริมสร้างความมั่นใจและความเชื่อมั่นระหว่างส่วนงาน อย่างต่อเนื่อง

๔.๓.๑.๒ ให้ความสำคัญกับการควบคุมและดำเนินการตามธรรมาภิบาลข้อมูลในทุกขั้นตอนวงจรชีวิตข้อมูล รวมทั้งบันทึกประวัติ เพื่อการตรวจสอบย้อนหลัง อันเป็นการประกันความเชื่อมั่นและโปร่งใสของการดำเนินงาน

๔.๓.๑.๓ ขับเคลื่อนกลไกธรรมาภิบาลข้อมูล ให้ทุกส่วนงาน รวมทั้งบุคลากรทุกระดับ มีส่วนร่วมในการดำเนินการอย่างเป็นระบบ และประสานสอดคล้อง

๔.๓.๒ นโยบายบูรณาการข้อมูลระหว่างหน่วยงาน

๔.๓.๒.๑ ส่งเสริมการบูรณาการข้อมูล รวมทั้งขับเคลื่อน ประสานงาน และประเมินผลการธรรมาภิบาลด้านการบูรณาการ ให้เป็นไปตามกรอบแนวทางธรรมาภิบาลข้อมูลภาครัฐ กฎหมาย และระเบียบที่เกี่ยวข้อง เพื่อเสริมสร้างความมั่นใจและความเชื่อมั่นระหว่างหน่วยงานของรัฐและภาคเอกชนที่เกี่ยวข้องอย่างต่อเนื่อง

๔.๓.๒.๒ ให้ความสำคัญกับการควบคุมและตรวจสอบการดำเนินการเพื่อให้การบูรณาการข้อมูลกับหน่วยงานของรัฐและภาคเอกชน เป็นไปตามธรรมาภิบาลข้อมูลในทุกขั้นตอนของวงจรชีวิตข้อมูล มีความโปร่งใส ชัดเจน และเป็นที่ยอมรับ

๔.๓.๒.๓ พัฒนาและเสริมสร้าง ความสัมพันธ์ ความตระหนักรู้ ความเข้าใจ การประสานความร่วมมือ และการแก้ไขปัญหาเพื่อสนับสนุนการบูรณาการข้อมูลระหว่างหน่วยงานของรัฐและภาคเอกชน โดยพัฒนาเป็นกรอบข้อตกลง มาตรฐาน รวมทั้งแนวปฏิบัติในทุกขั้นตอนวงจรชีวิตข้อมูล เพื่อให้เกิดการใช้ประโยชน์จากข้อมูลขนาดใหญ่ร่วมกัน อย่างสร้างสรรค์ และเป็นไปตามกรอบธรรมาภิบาลข้อมูล

๔.๓.๓ นโยบายการบริหารจัดการความเสี่ยง

๔.๓.๓.๑ กอ.รมน. ให้ความสำคัญและระมัดระวังผลกระทบอันเนื่องมากจากความผิดพลาดในการดำเนินการต่อข้อมูล ทั้งที่เป็นแบบเจตนาและไม่เจตนา อันก่อให้เกิดความเสียหายต่อองค์กร ทั้งทางตรงและทางอ้อม โดยกำหนดให้มีการประเมินความเสี่ยงอย่างเป็นวงรอบ และกำหนดเป็นแนวปฏิบัติเพื่อป้องกันปัญหาที่อาจเกิดขึ้น

๔.๓.๓.๒ เสริมสร้างความมั่นคงปลอดภัย ทั้งในเรื่องบุคคล เอกสาร สถานที่ ระบบเครือข่ายคอมพิวเตอร์และเทคโนโลยีสารสนเทศ และการรักษาความมั่นคงปลอดภัยไซเบอร์ เพื่อป้องกันการรั่วไหล การจารกรรม การก่อวินาศกรรม การบ่อนทำลาย การก่อการร้าย การกระทำที่เป็นภัยต่อความมั่นคงและผลประโยชน์แห่งรัฐ

๔.๓.๓.๓ ไม่เปิดเผย หรือส่งต่อ หรือถ่ายโอนข้อมูลที่บูรณาการมาจากส่วนงานหรือหน่วยงานของรัฐและภาคเอกชน (ทั้งที่เป็นข้อมูลทั่วไปและข้อมูลที่มีชั้นความลับ) ให้กับหน่วยงานหรือบุคคลอื่นโดยเด็ดขาด ยกเว้นกรณีดังต่อไปนี้

๔.๓.๓.๓ (๑) เป็นความต้องการของหน่วยเจ้าของข้อมูลที่มีหนังสือยืนยันเป็นลายลักษณ์อักษร

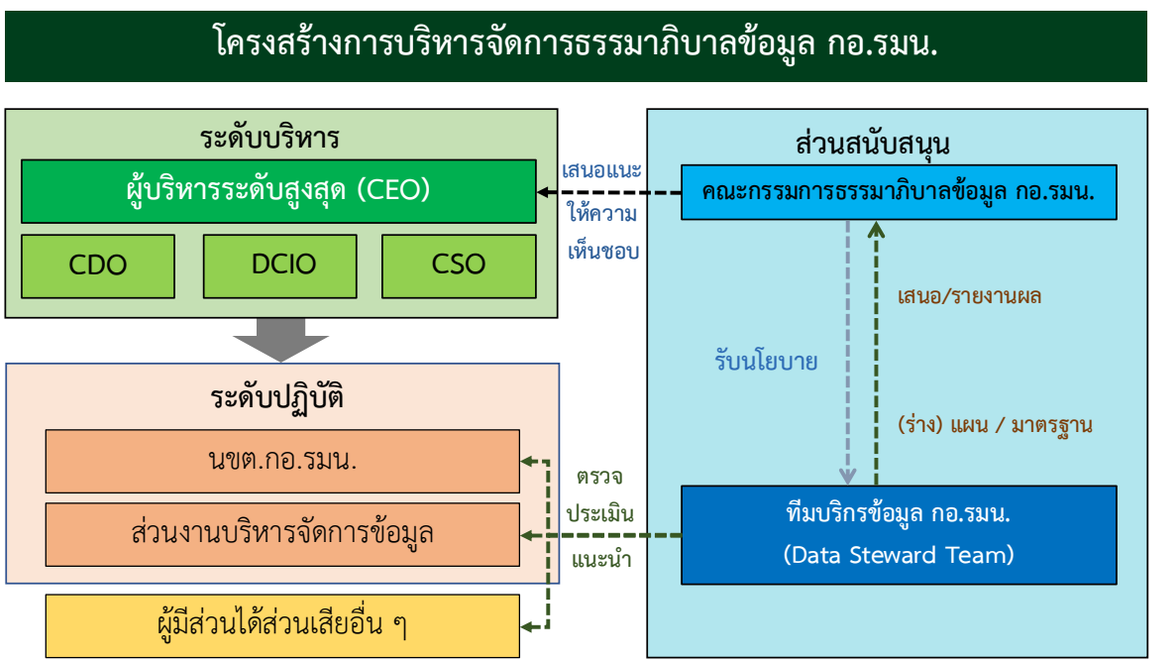
๔.๓.๓.๓ (๒) เป็นข้อมูลที่ผ่านการวิเคราะห์ประมวลผลข้อมูลขนาดใหญ่และนำเสนอในเนื้อหาที่มีเนื้อหาใหม่ ไม่เกี่ยวข้องกับข้อมูลส่วนบุคคล

๔.๔ โครงสร้างบุคลากรที่เกี่ยวข้องกับธรรมาภิบาลข้อมูล

กำหนดโครงสร้างและความรับผิดชอบของบุคลากรซึ่งเป็นผู้ที่มีส่วนได้ส่วนเสีย (Stakeholders) ต่อธรรมาภิบาลข้อมูล แบ่งเป็น ๓ ส่วน ตามรูปที่ ๔.๒ ดังนี้

๔.๔.๑ โครงสร้างและความรับผิดชอบของบุคลากรระดับบริหาร

๔.๔.๑.๑ ผู้บริหารระดับสูงสุด (Chief Executive Officer : CEO) กอ.รมน. รับผิดชอบในการกำหนดวิสัยทัศน์ ตัดสินใจและอนุมัตินโยบายข้อมูล มาตรฐานข้อมูล แนวทางปฏิบัติงาน เกณฑ์การวัดคุณภาพ ระเบียบ และข้อบังคับอื่น ๆ ที่เกี่ยวข้องกับข้อมูล รวมไปถึงการจัดลำดับความสำคัญในการแก้ไขปัญหาที่เกี่ยวข้องกับข้อมูล



รูปที่ ๔.๒ โครงสร้างบุคลากรที่เกี่ยวข้องกับธรรมาภิบาลข้อมูล กอ.รมน.

๔.๔.๑.๒ ผู้บริหารเทคโนโลยีสารสนเทศระดับสูงของ กอ.รมน. (Department Chief Information Officer : DCIO) รับผิดชอบ ดังนี้

๔.๔.๑.๒ (๑) เสนอแนะเป้าหมายและแนวทางการพัฒนารัฐบาลดิจิทัลของ กอ.รมน. กำกับการจัดทำสถาปัตยกรรมองค์กร แผนงาน โครงการ และงบประมาณ เพื่อการพัฒนารัฐบาลดิจิทัลของ กอ.รมน. รวมทั้งกำกับการบริหารจัดการโครงการ และการบริหารจัดการทรัพยากร เพื่อการใช้ประโยชน์ร่วมกัน

๔.๔.๑.๒ (๒) ส่งเสริม ผลักดัน และดำเนินการให้มีการปรับเปลี่ยนรูปแบบการให้บริการ และการทำงานภาครัฐของ กอ.รมน. ให้มีความทันสมัย โดยการนำเทคโนโลยีและข้อมูลมาใช้ในการสรรสร้างนวัตกรรมการบริการ และปรับปรุงรูปแบบ วิธีการ และกระบวนการทำงาน ให้มีประสิทธิภาพ โปร่งใส เชื่อมโยงระหว่างหน่วยงานทั้งภายในและภายนอกแบบอัตโนมัติ

๔.๔.๑.๒ (๓) กำกับดูแลการพัฒนาระบบงาน และโครงสร้างพื้นฐานด้านดิจิทัลของ กอ.รมน. ให้เป็นไปในแนวทางเดียวกัน มีประสิทธิภาพ เชื่อมโยง ไม่ซ้ำซ้อน สามารถนำมาต่อยอด และใช้ประโยชน์ร่วมกันได้

๔.๔.๑.๒ (๔) กำกับดูแลการพัฒนาดิจิทัลภายใน กอ.รมน. ให้เป็นตามหลักธรรมาภิบาล รวมทั้งจัดให้มีการบริหารจัดการความเสี่ยงและการเปลี่ยนแปลงเพื่อการป้องกันและแก้ไขปัญหาอย่างทันท่วงที และเพื่อให้เกิดการพัฒนาต่อยอดที่ยั่งยืน

๔.๔.๑.๒ (๕) ติดตาม สำรวจ และรายงานสถานการณ์การพัฒนารัฐบาลดิจิทัลของ กอ.รมน. ให้คณะกรรมการหรือผู้ที่เกี่ยวข้องได้ทราบ

๔.๔.๑.๒ (๖) กำกับ ให้คำปรึกษาแนะนำ และส่งเสริมสนับสนุนการพัฒนาบุคลากรให้มีทักษะด้านดิจิทัลในการปฏิบัติงาน การพัฒนานวัตกรรม และการทำงานร่วมกัน รวมทั้งพัฒนาระบบนิเวศและวัฒนธรรมองค์กรเพื่อสนับสนุนการพัฒนารัฐบาลดิจิทัลที่ต่อเนื่องและยั่งยืน

๔.๔.๑.๓ ผู้บริหารข้อมูลระดับสูงของ กอ.รมน. (Chief Data Officer : CDO) รับผิดชอบ ดังนี้

๔.๔.๑.๓ (๑) กำกับดูแลการจัดทำยุทธศาสตร์ แผนงาน และดำเนินการธรรมาภิบาลข้อมูล ให้มีคุณภาพ รวมทั้งสนับสนุนการดำเนินการด้านอื่น ๆ เพื่อรักษาความสมบูรณ์ และความเป็นส่วนบุคคลของข้อมูล

๔.๔.๑.๓ (๒) ควบคุมการนำเข้าและวิเคราะห์ข้อมูล เพื่อสร้างและส่งมอบเทคโนโลยี เครื่องมือ แนวทาง และวิธีการในการทำให้ข้อมูลมีคุณค่า และเกิดประโยชน์สูงสุดต่อ กอ.รมน. และหน่วยงานความมั่นคงที่เกี่ยวข้อง รวมทั้งส่งเสริมให้หน่วยงานของรัฐอื่น ๆ สามารถเข้าใช้งานข้อมูลได้อย่างถูกต้องและมีประสิทธิภาพ

๔.๔.๑.๓ (๓) เป็นแกนกลางในการประสานงานเพื่อให้เกิดการเชื่อมโยงแลกเปลี่ยนข้อมูลกับหน่วยงานภาครัฐอื่น ๆ รวมไปถึงการบริหารจัดการความเสี่ยงที่อาจเกิดขึ้น

๔.๔.๑.๓ (๔) ส่งเสริมนวัตกรรมที่ใช้ประโยชน์จากข้อมูล การนำข้อมูลไปใช้วิเคราะห์เพื่อการแก้ไขปัญหา และ/หรือ ลดความเสี่ยงการเกิดปัญหาที่อาจเกิดขึ้น รวมถึงการพิจารณาปรับปรุงเทคโนโลยีเพื่อการวิเคราะห์ข้อมูลให้มีความทันสมัย เหมาะสม และตอบสนองความต้องการของประชาชน

๔.๔.๑.๔ ผู้บริหารด้านการรักษาความปลอดภัยระดับสูงของ กอ.รมน. (Chief Security Officer : CSO) รับผิดชอบ ดังนี้

๔.๔.๑.๔ (๑) กำกับดูแลการดำเนินการทั้งปวง เพื่อให้โครงสร้างพื้นฐานด้านดิจิทัล ระบบงานสารสนเทศและข้อมูลที่อยู่ในความรับผิดชอบ และ/หรือ ข้อมูลที่มีความเกี่ยวข้องกับ กอ.รมน. มีความมั่นคงปลอดภัย

๔.๔.๑.๔ (๒) จัดลำดับความสำคัญเร่งด่วน วางแผน กำหนดเป้าหมายและวัตถุประสงค์ของการป้องกันและรักษาความมั่นคงปลอดภัย ให้สอดคล้องกับแผนปฏิบัติราชการ กอ.รมน.

๔.๔.๑.๔ (๓) ปรับปรุงพัฒนาขีดความสามารถด้านความมั่นคงปลอดภัยของ กอ.รมน. ทั้งทางด้านกายภาพและเทคโนโลยี

๔.๔.๑.๔ (๔) บูรณาการ ประสานการปฏิบัติด้านความมั่นคงปลอดภัย ร่วมกับคณะกรรมการ หน่วยงานและผู้บริหารของ กอ.รมน. และหน่วยงานภาครัฐอื่น ๆ

๔.๔.๑.๕ คณะกรรมการธรรมาภิบาลข้อมูล กอ.รมน. (ISOC Data Governance Council) มีองค์ประกอบ ได้แก่ ผู้บริหารระดับสูงสุด กอ.รมน. เป็นประธาน และมีผู้บริหารเทคโนโลยีสารสนเทศระดับสูง ผู้บริหารข้อมูล ผู้บริหารด้านการรักษาความปลอดภัยระดับสูง หัวหน้าส่วนงานใน กอ.รมน. ร่วมเป็นกรรมการ รับผิดชอบดังนี้

๔.๔.๑.๕ (๑) จัดทำธรรมาภิบาลข้อมูล กอ.รมน. เพื่อใช้เป็นกลไกในการขับเคลื่อนการบริหารจัดการข้อมูลภายใน กอ.รมน. และข้อมูลของหน่วยงานภาครัฐอื่น ๆ ที่นำเข้ามาใช้งานภายใน กอ.รมน. ให้มีความสอดคล้องกับนโยบายรัฐบาล ยุทธศาสตร์ชาติประเด็นความมั่นคง และกฎหมายที่เกี่ยวข้อง

๔.๔.๑.๕ (๒) พิจารณาให้ความเห็นชอบนโยบาย มาตรฐาน สิทธิ และแนวปฏิบัติที่เกี่ยวข้องกับธรรมาภิบาลข้อมูลของ กอ.รมน.

๔.๔.๑.๕ (๓) ควบคุม ติดตาม กำกับดูแล และประเมินการดำเนินการตามธรรมาภิบาลข้อมูลของ กอ.รมน. รวมทั้งความปลอดภัย และคุณภาพข้อมูลให้เป็นไปตามนโยบายและมาตรฐานข้อมูลของ กอ.รมน.

๔.๔.๑.๖ ทีมบริกรข้อมูล กอ.รมน. (ISOC Data Steward Team) มีผู้อำนวยการศูนย์ดิจิทัลเพื่อความมั่นคง กอ.รมน. เป็นหัวหน้าทีม และมีผู้อำนวยการส่วนของสำนักฝ่ายอำนวยการที่เกี่ยวข้องกับงานบริกรข้อมูลร่วมเป็นทีมงาน รับผิดชอบ ดังนี้

๔.๔.๑.๖ (๑) รวบรวมข้อมูลเพื่อนำไปใช้ประกอบการกำหนด (ร่าง) นโยบาย มาตรฐาน และแนวปฏิบัติ ความปลอดภัย และคุณภาพข้อมูล จากผู้มีส่วนได้ส่วนเสียกับข้อมูล (Data Stakeholders)

๔.๔.๑.๖ (๒) พิจารณาจัดทำ (ร่าง) นโยบาย มาตรฐาน การกำหนดสิทธิ หน้าที่ และแนวปฏิบัติที่เกี่ยวข้องกับธรรมาภิบาลข้อมูลของ กอ.รมน.

๔.๔.๑.๖ (๓) ให้ข้อมูลสนับสนุนการตัดสินใจของคณะกรรมการธรรมาภิบาลข้อมูล กอ.รมน. รวมทั้งรับนโยบาย เพื่อนำไปสู่การปฏิบัติ ภายใต้บทบาทการเป็นบริกรข้อมูลที่มีความรู้ ทักษะ

๔.๔.๑.๖ (๔) ประเมินความพร้อมการธรรมาภิบาลข้อมูลของ กอ.รมน.

๔.๔.๑.๖ (๕) ขับเคลื่อน ตรวจสอบ ประเมินและรายงานผลการปฏิบัติตามนโยบายและแนวปฏิบัติตามที่กำหนดในธรรมาภิบาลข้อมูล กอ.รมน. รวมทั้งความปลอดภัยและคุณภาพของข้อมูลให้คณะกรรมการธรรมาภิบาลข้อมูล กอ.รมน. ตามห้วงเวลาที่เหมาะสม

๔.๔.๑.๗ ผู้เชี่ยวชาญเฉพาะทาง (Domain Expert) เป็นบุคลากรที่มีความรู้ ประสบการณ์ รวมทั้งความชำนาญในการใช้ประโยชน์เกี่ยวกับข้อมูลด้านใดด้านหนึ่งเป็นการเฉพาะ ทั้งนี้ บุคลากรดังกล่าวอาจเป็นบุคลากรของ กอ.รมน. หรือ หน่วยงานของรัฐ หรือภาคเอกชน ก็ได้ โดยมีทีมบริกรข้อมูลเป็นผู้แต่งตั้งและมอบหมายภารกิจ ทั้งนี้หน้าที่สำคัญของผู้เชี่ยวชาญเฉพาะทาง ได้แก่ การให้คำแนะนำเพื่อกำหนดเป้าหมาย ทิศทางความต้องการนำข้อมูลขนาดใหญ่ ไปใช้ประโยชน์ให้กับทีมบริกรข้อมูล รวมทั้งสนับสนุนการดำเนินการเพื่อวิเคราะห์ประมวลผลข้อมูล สนับสนุนส่วนงานบริหารจัดการข้อมูล และนักวิเคราะห์ข้อมูล เป็นต้น

๔.๔.๒ โครงสร้างและความรับผิดชอบของบุคลากรระดับปฏิบัติ

๔.๔.๒.๑ ผู้ควบคุมข้อมูลส่วนบุคคล (Data Controller) กอ.รมน. หมายถึง สำนักนายกรัฐมนตรี ซึ่งอาจมอบหมายให้ กอ.รมน. โดยผู้บริหารข้อมูลระดับสูง กอ.รมน. เป็นผู้รับผิดชอบ โดยมีหน้าที่และอำนาจในการตัดสินใจเกี่ยวกับการเก็บ รวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล รวมถึงการบริหารจัดการ การกำหนดรายละเอียดวัตถุประสงค์ ระเบียบวิธีดำเนินการ และการกำกับดูแลการปฏิบัติด้านข้อมูลส่วนบุคคลทั้งปวงของ กอ.รมน. โดยต้องจัดให้มีเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล ตามที่กฎหมายได้บัญญัติไว้ เพื่อดำเนินการให้เป็นไปตามนโยบายและแนวปฏิบัติที่ธรรมาภิบาลข้อมูลด้านความมั่นคงของ กอ.รมน. ฉบับนี้กำหนด

๔.๔.๒.๒ ผู้ประมวลผลข้อมูลส่วนบุคคล (Data Processor) หมายถึง สำนักนายกรัฐมนตรี ซึ่งอาจมอบหมายให้ กอ.รมน. โดยส่วนงานบริหารจัดการข้อมูล หรือนิติบุคคลใด ๆ รับผิดชอบการดำเนินการเกี่ยวกับการเก็บ รวบรวม ใช้ หรือเปิดเผยข้อมูลที่มิใช่ข้อมูลส่วนบุคคล ตามคำสั่งหรือในนามของผู้ควบคุมข้อมูลส่วนบุคคล

๔.๔.๒.๓ เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (Data Protection Officer) เป็นบุคคลหรือกลุ่มบุคคล ที่ได้รับการแต่งตั้งโดยผู้ควบคุมข้อมูลส่วนบุคคล ให้มีหน้าที่และอำนาจในการตรวจสอบการดำเนินงานเกี่ยวกับข้อมูลส่วนบุคคลทั้งปวง ได้แก่การรวบรวม จัดเก็บ ใช้ เผยแพร่ เปิดเผย จัดเก็บถาวร ทำลาย และการดำเนินการใด ๆ ต่อข้อมูลส่วนบุคคลที่อยู่ในความรับผิดชอบของผู้ควบคุมข้อมูลส่วนบุคคล

๔.๔.๒.๔ ส่วนงานเจ้าของข้อมูล หมายถึง ส่วนงานใน กอ.รมน. ที่ครอบครองข้อมูลในแต่ละขั้นตอนของวงจรชีวิตข้อมูลที่อยู่ในกรอบความรับผิดชอบของ กอ.รมน. และต้องรับผิดชอบต่อข้อมูลดังกล่าวตามที่กฎหมายกำหนด ได้แก่ การกำหนดให้ปฏิบัติหรือไม่ให้ปฏิบัติการใด ๆ กับข้อมูลที่เป็นเจ้าของ การกำหนดข้อตกลงในการให้ใช้หรือไม่ให้ใช้ข้อมูลในการบูรณาการข้อมูลของตน การกำหนดชั้นความลับของข้อมูล รวมทั้งมีหน้าที่แจ้งเจ้าของข้อมูลส่วนบุคคล เพื่อทราบกรณีเกิดเหตุการณ์ที่ส่งผลกระทบหรืออาจส่งผลกระทบต่อเจ้าของข้อมูลส่วนบุคคล ทั้งนี้หัวหน้าส่วนงานเจ้าของข้อมูล อาจพิจารณาแต่งตั้งเจ้าหน้าที่คุ้มครองข้อมูล ผู้ควบคุมข้อมูล ผู้ควบคุมข้อมูลส่วนบุคคล วิศวกรระบบ วิศวกรข้อมูล นักวิเคราะห์ข้อมูล วิศวกรความมั่นคงปลอดภัยไซเบอร์ ของส่วนงานตนเอง เป็นรายกรณีได้ (หากมีความจำเป็น)

๔.๔.๒.๕ ส่วนงานบริหารจัดการข้อมูล หมายถึง หน่วยปฏิบัติในการบริหารจัดการข้อมูลที่ได้เชื่อมโยงแลกเปลี่ยนเข้ามาจากส่วนงาน หน่วยงานของรัฐ หรือภาคเอกชน โดยมีศูนย์ดิจิทัลเพื่อความมั่นคง กอ.รมน. ในฐานะศูนย์กลางข้อมูลด้านความมั่นคง รับผิดชอบในการวางแผน อำนวยการและประสานการปฏิบัติในการเชื่อมโยงแลกเปลี่ยนข้อมูล ดำเนินการ ตรวจสอบ และประเมินผลการบริหารจัดการข้อมูลระดับบูรณาการ รวมถึงเครื่องมือที่ใช้สนับสนุนการดำเนินงานทางด้านเทคนิค ของ กอ.รมน.

๔.๔.๒.๖ วิศวกรระบบ (System Engineer) เป็นเจ้าหน้าที่ขึ้นตรงกับส่วนงานบริหารจัดการข้อมูล รับผิดชอบเกี่ยวกับการพัฒนา บริหารจัดการ และควบคุมการใช้งานทั้งปวงที่เกี่ยวกับโครงสร้างพื้นฐานด้านดิจิทัลของ กอ.รมน. รวมถึงโครงสร้างพื้นฐานด้านดิจิทัลที่ใช้สนับสนุนงานบูรณาการและการบริหารจัดการข้อมูล ได้แก่ ระบบฐานข้อมูลกลาง บิ๊กดาต้าแพลตฟอร์ม ระบบเครือข่าย และระบบเชื่อมโยงแลกเปลี่ยนข้อมูล เป็นต้น

๔.๔.๒.๗ วิศวกรข้อมูล (Data Engineer) เป็นเจ้าหน้าที่ขึ้นตรงกับส่วนงานบริหารจัดการข้อมูล รับผิดชอบเกี่ยวกับการพัฒนา โครงสร้าง สถาปัตยกรรม และความสัมพันธ์ระหว่างข้อมูลระดับบูรณาการ รวมทั้งบริหารจัดการและกำกับดูแลการเชื่อมโยงข้อมูลให้เป็นข้อมูลขนาดใหญ่ ผ่านขั้นตอนการดำเนินการทั้งปวงในวงจรชีวิตข้อมูล

๔.๔.๒.๘ นักวิเคราะห์ข้อมูล (Data Analyst) เป็นเจ้าหน้าที่ขึ้นตรงกับส่วนงานบริหารจัดการข้อมูล รับผิดชอบเกี่ยวกับการรวบรวม ศึกษาข้อมูลภายในข้อมูลขนาดใหญ่ เพื่อเชื่อมโยงความสัมพันธ์ สร้างแบบจำลอง หรือนำเทคโนโลยีการเรียนรู้ของเครื่อง และปัญญาประดิษฐ์ มาใช้สนับสนุนการวิเคราะห์ประมวลผลและการนำไปใช้ประโยชน์ในด้านต่าง ๆ

๔.๔.๒.๙ วิศวกรความมั่นคงปลอดภัยไซเบอร์ (Cyber Security Engineer) เป็นเจ้าหน้าที่ขึ้นตรงกับส่วนงานบริหารจัดการข้อมูล รับผิดชอบเกี่ยวกับการป้องกันและรักษาความมั่นคงปลอดภัยเกี่ยวกับข้อมูล การเชื่อมโยงแลกเปลี่ยนข้อมูล และโครงสร้างพื้นฐานด้านดิจิทัลที่ใช้สนับสนุนงานบูรณาการและการบริหารจัดการข้อมูล

๔.๔.๒.๑๐ ทีมบริหารจัดการข้อมูล หมายถึง กลุ่มเจ้าหน้าที่ที่ส่วนงานของ กอ.รมน. หรือส่วนงานบริหารจัดการข้อมูล ได้แต่งตั้งและมอบหมายหน้าที่และอำนาจเกี่ยวกับงานบริหารจัดการข้อมูลที่อยู่ในความรับผิดชอบ ครอบคลุมงานวิศวกรระบบ วิศวกรข้อมูล นักวิเคราะห์ข้อมูล และวิศวกรความมั่นคงปลอดภัยไซเบอร์

๔.๔.๒.๑๑ เจ้าหน้าที่บริหารจัดการข้อมูล หมายถึง เจ้าหน้าที่ที่ส่วนงานของ กอ.รมน. หรือส่วนงานบริหารจัดการข้อมูล ได้แต่งตั้งและมอบหมายหน้าที่และอำนาจเกี่ยวกับงานบริหารจัดการข้อมูลที่อยู่ในความรับผิดชอบ ครอบคลุมงานวิศวกรระบบ วิศวกรข้อมูล นักวิเคราะห์ข้อมูล และวิศวกรความมั่นคงปลอดภัยไซเบอร์ (ในกรณีที่ส่วนงานของ กอ.รมน. ไม่สามารถจัดตั้งทีมบริหารจัดการข้อมูลได้)

๔.๔.๓ ความรับผิดชอบของผู้ที่มีส่วนได้ส่วนเสียอื่น ๆ

เนื่องจากผู้ที่มีส่วนได้ส่วนเสีย มีความเกี่ยวข้องกับนโยบายและมาตรฐานข้อมูล รวมทั้งแนวปฏิบัติการธรรมาภิบาลข้อมูลของ กอ.รมน. ทั้งทางตรงและทางอ้อม ดังนั้น จึงมีส่วนงานหรือบุคคลอื่น ๆ นอกเหนือจากที่ได้กล่าวในข้อ ๔.๔.๑ - ๔.๔.๒ ดังนี้

๔.๔.๓.๑ หน่วยงานเจ้าของข้อมูล หมายถึง หน่วยงานของรัฐ หรือภาคเอกชน ที่ครอบครองข้อมูลในแต่ละขั้นตอนของวงจรชีวิตข้อมูล และต้องรับผิดชอบต่อข้อมูลดังกล่าวตามที่กฎหมายกำหนด ได้แก่ การกำหนดให้ปฏิบัติหรือไม่ให้ปฏิบัติการใด ๆ กับข้อมูลที่เป็นเจ้าของ การกำหนดข้อตกลงในการให้ใช้หรือไม่ให้ใช้ข้อมูลในการบูรณาการข้อมูลของตน การกำหนดชั้นความลับของข้อมูล รวมทั้งมีหน้าที่แจ้งเจ้าของข้อมูลส่วนบุคคล เพื่อทราบกรณีเกิดเหตุการณ์ที่ส่งผลกระทบหรืออาจส่งผลกระทบต่อเจ้าของข้อมูลส่วนบุคคล เป็นต้น

๔.๔.๓.๒ ผู้สร้างข้อมูล (Data Creators) หมายถึง บุคคล หรืออุปกรณ์ หรือระบบงานใด ๆ ที่มีบทบาทในการสร้าง จัดเก็บ แก้ไข ปรับปรุง หรือลบข้อมูลในแต่ละขั้นตอนของวงจรชีวิตข้อมูลที่อยู่ในความรับผิดชอบของ กอ.รมน. นอกจากนั้น ผู้สร้างข้อมูลยังมีหน้าที่ในการสนับสนุนการทำงานร่วมกับทีมบริกรข้อมูล เพื่อตรวจสอบและแก้ไขปัญหาด้านคุณภาพข้อมูลและความปลอดภัยของข้อมูล หรือรายงานประเด็นปัญหาที่ตรวจพบระหว่างการสร้างข้อมูล ให้หน่วยงานและผู้ที่เกี่ยวข้องทราบ

๔.๔.๓.๓ ผู้ใช้งานข้อมูล (Data User) หมายถึง บุคลากรหรือส่วนงานของกอ.รมน. หรือหน่วยงานของรัฐหรือภาคเอกชน (ทั้งในระดับบริหารหรือระดับปฏิบัติ) หรือประชาชนทั่วไป ที่มีสิทธิหรือได้รับอนุญาตให้นำข้อมูลไปประมวลผลหรือใช้งาน โดยมีหน้าที่ดำเนินการและกำกับดูแลเกี่ยวกับข้อมูล ให้เป็นไปตามนโยบาย และแนวปฏิบัติในการธรรมาภิบาลข้อมูลของ กอ.รมน. รวมถึงการรายงานประเด็นปัญหาที่ตรวจพบระหว่างการใช้ ทั้งในด้านความปลอดภัยและคุณภาพของข้อมูล ให้หน่วยงานและผู้ที่เกี่ยวข้องทราบ

๔.๔.๓.๔ เจ้าของข้อมูลส่วนบุคคล (Data Subject) หมายถึง บุคคลใด ๆ ที่ข้อมูลสามารถระบุไปถึงตัวตนของบุคคลนั้นได้

๔.๕ นิยามศัพท์ด้านธรรมาภิบาลข้อมูล

เพื่อให้การดำเนินการต่อข้อมูลภายใต้กรอบธรรมาภิบาลข้อมูล มีความชัดเจน สามารถสื่อสารระหว่างผู้เกี่ยวข้อง ได้อย่างมีประสิทธิภาพ จึงกำหนดนิยามศัพท์ที่เกี่ยวข้องกับข้อมูล ไว้ดังนี้

๔.๕.๑ “ชุดข้อมูล (Datasets)” หมายถึง ข้อมูลที่มีการรวบรวมไว้ โดยปกติอยู่ในรูปแบบของตารางข้อมูล ซึ่งการรวบรวมข้อมูลนี้มาจากหลายแหล่ง และนำข้อมูลมาจัดเป็นชุดให้ถูกต้องตามลักษณะโครงสร้างข้อมูลที่กำหนดไว้

๔.๕.๒ “ข้อมูลหลัก (Master Data)” หมายถึง ข้อมูลที่มีโอกาสเปลี่ยนแปลงได้มากกว่า มีรายละเอียดหรือจำนวนฟิลด์ข้อมูลที่มากกว่า และใช้เป็นข้อมูลในการดำเนินงานภายในส่วนงาน เช่น ข้อมูลพนักงาน ข้อมูลลูกค้า ข้อมูลผู้ขาย ข้อมูลสินค้า ข้อมูลครุภัณฑ์ ข้อมูลสถานที่ เป็นต้น

๔.๕.๓ “ข้อมูลอ้างอิง (Reference Data)” หมายถึง ข้อมูลที่เป็นสากล มีการเปลี่ยนแปลงค่อนข้างน้อย เช่น รหัสไปรษณีย์ รหัสประเทศ หน่วยวัดระยะทาง เป็นต้น

๔.๕.๔ “ชุดข้อมูลดิจิทัล หรือเมทาดาตา (Metadata)” หมายถึง ข้อมูลที่ใช้อธิบายข้อมูลหลักหรือกลุ่มข้อมูลอื่น ๆ ที่เกี่ยวข้องทั้งกระบวนการเชิงภารกิจและเชิงเทคโนโลยีสารสนเทศ กฎและข้อจำกัดของข้อมูล และโครงสร้างของข้อมูล

๔.๕.๕ “ข้อมูลนิรนาม (Anonymous Data)” หมายถึง ข้อมูลส่วนบุคคลที่ผ่านการทำให้ข้อมูลมีความเสี่ยงในการระบุตัวตนของเจ้าของข้อมูลได้น้อยมากจนแทบจะถือว่าไม่มีความเสี่ยง (Data Anonymization) เช่น การเข้ารหัสและเปลี่ยนแปลงข้อมูลให้เป็นอื่นด้วยวิธีการทางเทคนิค

๔.๕.๖ “ข้อมูลแฝง (Pseudonymous Data)” หมายถึง ข้อมูลที่ผ่านกระบวนการแฝงข้อมูล (Data Pseudonymization) ที่มีการประมวลผลข้อมูลส่วนบุคคลในลักษณะที่เป็นการลดหรือจำกัดความสามารถในการเชื่อมโยงข้อมูลส่วนบุคคลกับชุดข้อมูลตั้งต้นทำให้ข้อมูลส่วนบุคคลไม่สามารถระบุตัวเจ้าของข้อมูลได้หากปราศจากการใช้ข้อมูลเพิ่มเติมประกอบ ทั้งนี้ข้อมูลเพิ่มเติมนี้มีการเก็บรักษาไว้แยกออกจากกันและอยู่ภายใต้มาตรการเชิงเทคนิคและมาตรการเชิงบริหารจัดการเพื่อประกันว่าข้อมูลส่วนบุคคลจะไม่สามารถระบุไปถึงบุคคลธรรมดาได้

๔.๕.๗ “ข้อมูลรั่วไหล (Data Breach)” หมายถึง การที่ข้อมูลถูกละเมิดด้วยวิธีการเข้าถึง การเปิดเผย การแก้ไขเปลี่ยนแปลงข้อมูล การทำให้ข้อมูลสูญหาย การทำลายข้อมูล การส่งต่อ การเก็บรักษาหรือประมวลผลจากการกระทำโดยมิชอบด้วยกฎหมายหรือโดยอุบัติเหตุ

๔.๕.๘ “ข้อมูลส่วนบุคคล (Personal Data)” หมายถึง ข้อมูลเกี่ยวกับบุคคลซึ่งทำให้สามารถระบุตัวบุคคลนั้นได้ไม่ว่าทางตรงหรือทางอ้อม แต่ไม่รวมถึงข้อมูลของผู้ถึงแก่กรรมโดยเฉพาะ

๔.๕.๙ "ข้อมูลสาธารณะ (Public Data)” หมายถึง ข้อมูลที่สามารถเปิดเผยให้ประชาชนรับทราบได้และนำไปใช้ได้อย่างอิสระ ไม่ว่าจะเป็นข้อมูลข่าวสาร ข้อมูลส่วนบุคคล หรือข้อมูลอิเล็กทรอนิกส์ เป็นต้น อีกทั้งสามารถตรวจสอบได้โดยไม่จำเป็นต้องร้องขอ

๔.๕.๑๐ “ข้อมูลอ่อนไหว (Sensitive Personal Data)” หมายถึง ข้อมูลส่วนบุคคลที่เป็นเรื่องส่วนตัวโดยแท้ของบุคคล แต่มีความละเอียดอ่อนและสุ่มเสี่ยงต่อการถูกใช้ในการเลือกปฏิบัติอย่างไม่เป็นธรรม จึงจำเป็นต้องดำเนินการด้วยความระมัดระวังเป็นพิเศษ

๔.๕.๑๑ “บัญชีข้อมูล (Data Catalog)” หมายถึง เอกสารแสดงรายการของชุดข้อมูลที่จำแนกโดยการจัดกลุ่มหรือจัดประเภทข้อมูลที่อยู่ในความครอบครองหรือควบคุมของ กอ.รมน.

๔.๕.๑๒ “บัญชีคุมข้อมูล (Data Inventory)” หมายถึง เอกสารแสดงรายละเอียดของชุดข้อมูล แบ่งเป็นบัญชีคุมข้อมูลปกติ และบัญชีคุมข้อมูลพิเศษ รายละเอียดประกอบด้วย ส่วนตารางชื่อชุดข้อมูล หมายเลขชุดข้อมูล หมายเลขเจ้าของข้อมูล ประเภทข้อมูล รายละเอียดการจัดเก็บ และวันสิ้นอายุ

๔.๕.๑๓ “พจนานุกรมข้อมูล (Data Dictionary)” หมายถึง เอกสารที่ใช้สำหรับอธิบายรายละเอียดของชุดข้อมูล คำอธิบายความหมายของข้อมูลที่ระบุรายละเอียด Tables, Fields หรือ Columns, Data Types และคำอธิบายรายละเอียดข้อมูลและเงื่อนไขต่าง ๆ ของแต่ละ Fields และเป็นเอกสารสำหรับใช้อ้างอิงในการคำนวณ ประมวลผลและใช้เป็น Metadata ในการทำ Data Catalog

๔.๕.๑๔ “ข้อมูลที่มีโครงสร้าง (Structured Data)” เป็นข้อมูลที่มีการนิยามโครงสร้างของข้อมูลไว้โดยนิยามความหมายและคุณสมบัติของแต่ละฟิลด์ข้อมูล โครงสร้างมีชั้นเดียวทำให้ง่ายต่อการค้นหา เช่น ตารางข้อมูลในฐานข้อมูล CSV เป็นต้น

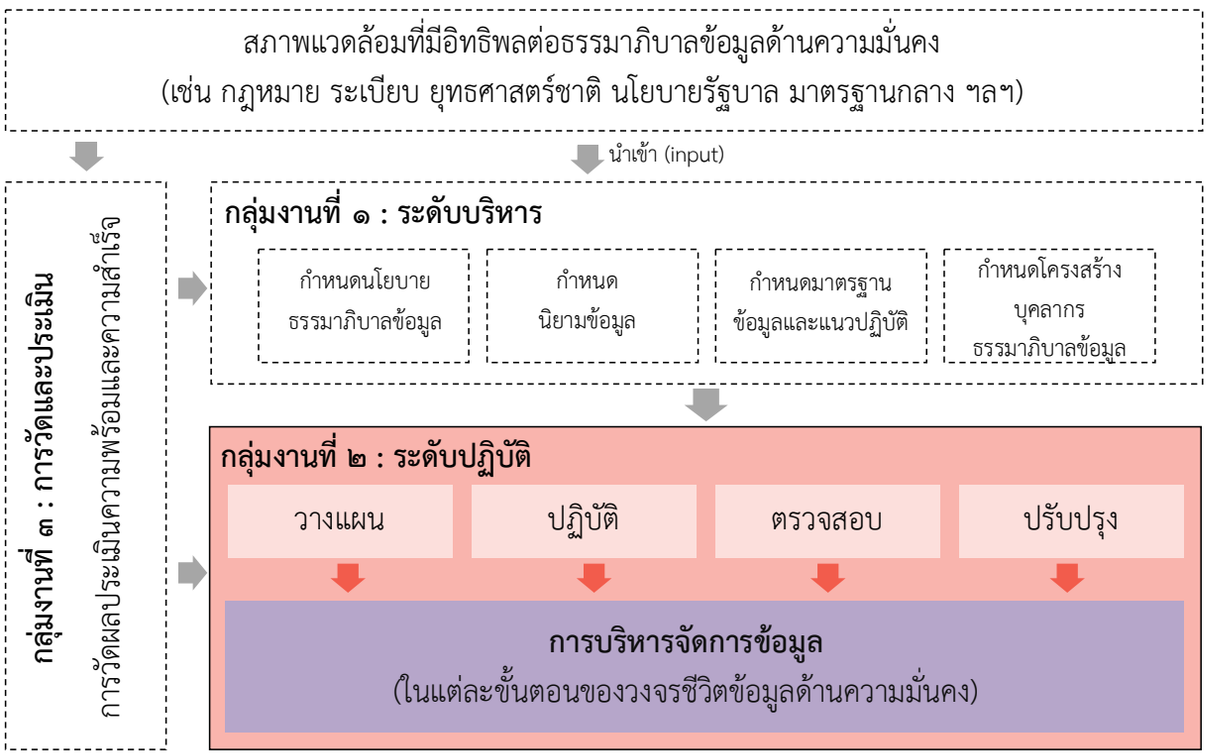
๔.๕.๑๕ “ข้อมูลกึ่งโครงสร้าง (Semi-structured Data)” เป็นข้อมูลที่มีการนิยามโครงสร้างของข้อมูลไว้แต่โครงสร้างเป็นแบบลำดับขั้น (Hierarchy) เช่น XML JSON เป็นต้น

๔.๕.๑๖ “ข้อมูลที่ไม่มีโครงสร้าง (Unstructured Data)” เป็นข้อมูลที่ไม่ได้มีการนิยามโครงสร้างของข้อมูลไว้ เช่น ข้อความ รูปภาพ เสียง และวีดิทัศน์ เป็นต้น

รูปที่ ๔.๓ ลักษณะของข้อมูลที่มีโครงสร้าง กึ่งโครงสร้าง และไม่มีโครงสร้าง

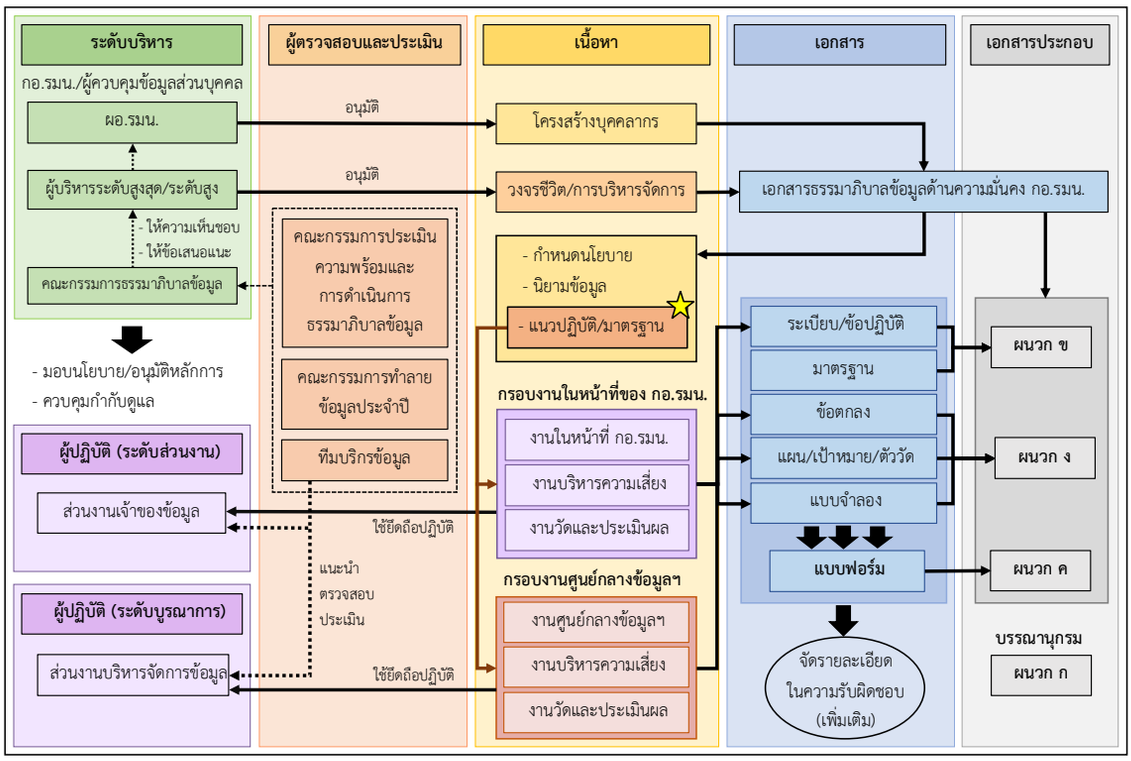
๔.๖ แนวปฏิบัติเพื่อขับเคลื่อนธรรมาภิบาลข้อมูล

การขับเคลื่อนงานธรรมาภิบาลข้อมูล ทั้งในมิติความรับผิดชอบตามหน้าที่และอำนาจของ กอ.รมน. และในบทบาทศูนย์กลางข้อมูลด้านความมั่นคง จำเป็นต้องกำหนดกรอบขอบเขตแนวปฏิบัติเพื่อขับเคลื่อนธรรมาภิบาลข้อมูลในระดับปฏิบัติ ให้เป็นไปตามนโยบายและแนวปฏิบัติในภาพรวม (ระดับบริหาร) ตามรูปที่ ๔.๔



รูปที่ ๔.๔ แนวปฏิบัติเพื่อขับเคลื่อนธรรมาภิบาลข้อมูลในระดับปฏิบัติ

โดยแบ่ง ออกเป็น ๔ ส่วน ประกอบด้วย (๑) ขอบเขตการธรรมาภิบาลข้อมูลในกรอบหน้าที่และอำนาจของ กอ.รมน. (๒) ขอบเขตการธรรมาภิบาลข้อมูลในกรอบความรับผิดชอบของศูนย์กลางข้อมูลด้านความมั่นคง (๓) ขอบเขตการบริหารจัดการความเสี่ยง และ (๔) ขอบเขตการวัดและประเมินผลการดำเนินการ รายละเอียดตามรูปที่ ๔.๕ ดังนี้



รูปที่ ๔.๕ ความสัมพันธ์ระหว่างบุคลากร ภาระงาน และเอกสารธรรมาภิบาลข้อมูลของ กอ.รมน.

๔.๖.๑ ขอบเขตการธรรมาภิบาลข้อมูลในกรอบหน้าที่และอำนาจของ กอ.รมน.

ให้ส่วนงานของ กอ.รมน. ที่มีฐานะเป็นเจ้าของข้อมูล กำหนดโครงสร้างบุคลากร รวมทั้งจัดทำมาตรฐานและแนวปฏิบัติการธรรมาภิบาลข้อมูลตามกรอบความรับผิดชอบของหน่วย ให้เป็นไปตามนโยบายและแนวปฏิบัติกลางที่เอกสารธรรมาภิบาลข้อมูลของ กอ.รมน. กำหนด และครอบคลุมขอบเขตงานที่เกี่ยวข้องทั้งระบบ โดยมีทีมบริกรข้อมูล กอ.รมน. สนับสนุนการปฏิบัติ ให้คำปรึกษา รวมทั้งตรวจสอบการปฏิบัติ ทั้งนี้ในกรณีที่เห็นว่าแนวปฏิบัติของส่วนงานใด ที่นำไปใช้งานและปรับปรุงจนมีความครบถ้วนสมบูรณ์ เป็นที่ยอมรับจากผู้มีส่วนได้ส่วนเสีย และเห็นว่าเป็นประโยชน์ต่อส่วนรวม ให้พิจารณาเสนอกำหนดเป็นแนวปฏิบัติหรือมาตรฐานกลางของ กอ.รมน. โดยมีขอบเขตงานที่ต้องดำเนินการ รวม ๕ เรื่อง ดังนี้

๔.๖.๑.๑ แนวปฏิบัติและมาตรฐานข้อมูลเกี่ยวกับการสร้างและจัดเก็บ

๔.๖.๑.๒ แนวปฏิบัติและมาตรฐานข้อมูลเกี่ยวกับใช้งาน

๔.๖.๑.๓ แนวปฏิบัติและมาตรฐานข้อมูลเกี่ยวกับการเผยแพร่

๔.๖.๑.๔ แนวปฏิบัติและมาตรฐานข้อมูลเกี่ยวกับจัดเก็บข้อมูลถาวร

๔.๖.๑.๕ แนวปฏิบัติและมาตรฐานข้อมูลเกี่ยวกับทำลาย

๔.๖.๒ ขอบเขตการธรรมาภิบาลข้อมูลในกรอบความรับผิดชอบของศูนย์กลางข้อมูลด้านความมั่นคง

เนื่องจากการดำเนินงานในมิติศูนย์กลางข้อมูลด้านความมั่นคง เกี่ยวข้องกับหน่วยงานของรัฐจำนวนมาก ดังนั้นการกำหนดโครงสร้างบุคลากร รวมทั้งจัดทำมาตรฐานและแนวปฏิบัติการธรรมาภิบาลข้อมูลจึงอยู่ในกรอบหน้าที่และอำนาจของผู้บริหารระดับสูงสุด (CEO) ของ กอ.รมน. โดยมีคณะกรรมการธรรมาภิบาล

ข้อมูลด้านความมั่นคง กอ.รมน. ซึ่งมีองค์ประกอบที่สำคัญ ได้แก่ ผู้บริหารเทคโนโลยีสารสนเทศระดับสูง (DCIO) ผู้บริหารข้อมูลระดับสูง (CDO) ผู้บริหารด้านการรักษาความปลอดภัยระดับสูง (CSO) รวมทั้งหัวหน้าส่วนงานของ กอ.รมน. ฯลฯ ทำหน้าที่พิจารณา กลั่นกรอง ให้ความเห็นชอบนโยบาย ระเบียบ มาตรฐาน และแนวปฏิบัติที่เกี่ยวข้องกับธรรมาภิบาลข้อมูลของ กอ.รมน. และมีส่วนงานบริหารจัดการข้อมูล (ศูนย์ดิจิทัลเพื่อความมั่นคง กอ.รมน.) เป็นระดับปฏิบัติในการจัดทำรายละเอียดมาตรฐานและแนวปฏิบัติภายในศูนย์กลางข้อมูลด้านความมั่นคงให้เป็นไปตามนโยบายและแนวปฏิบัติกลางที่เอกสารธรรมาภิบาลข้อมูลของ กอ.รมน. กำหนด และครอบคลุมขอบเขตงานที่เกี่ยวข้องทั้งระบบ โดยมีทีมบริกรข้อมูล กอ.รมน. สนับสนุนการปฏิบัติ ให้คำปรึกษา รวมทั้งตรวจสอบการปฏิบัติ ทั้งนี้ มีขอบเขตงานที่ส่วนงานบริหารจัดการข้อมูลต้องดำเนินการ รวม ๕ เรื่อง ดังนี้

๔.๖.๒.๑ แนวปฏิบัติและมาตรฐานข้อมูลเกี่ยวกับการบูรณาการ การเชื่อมโยงแลกเปลี่ยนข้อมูล

๔.๖.๒.๒ แนวปฏิบัติและมาตรฐานข้อมูลเกี่ยวกับใช้งานข้อมูลที่ได้จากการบูรณาการ

๔.๖.๒.๓ แนวปฏิบัติและมาตรฐานข้อมูลเกี่ยวกับการเผยแพร่ข้อมูลที่ได้จากการบูรณาการ

๔.๖.๒.๔ แนวปฏิบัติและมาตรฐานข้อมูลเกี่ยวกับจัดเก็บข้อมูลถาวรที่ได้จากการบูรณาการ

๔.๖.๒.๕ แนวปฏิบัติและมาตรฐานข้อมูลเกี่ยวกับทำลายข้อมูลที่ได้จากการบูรณาการ

๔.๖.๓ ขอบเขตการบริหารจัดการความเสี่ยง

ให้ส่วนงานของ กอ.รมน. ที่มีฐานะเป็นเจ้าของข้อมูล และส่วนงานบริหารจัดการข้อมูล (ศูนย์ดิจิทัลเพื่อความมั่นคง กอ.รมน.) กำหนดโครงสร้างบุคลากร รวมทั้งจัดทำมาตรฐานและแนวปฏิบัติการบริหารจัดการความเสี่ยง ให้เป็นไปตามนโยบายและแนวปฏิบัติกลางที่เอกสารธรรมาภิบาลข้อมูลของ กอ.รมน. กำหนด ให้ครอบคลุมระดับความเสี่ยงของข้อมูลที่อยู่ในความรับผิดชอบ ในทุกขั้นตอนของวงจรชีวิตข้อมูล โดยมีขอบเขตงานที่ต้องดำเนินการ รวม ๓ เรื่อง ดังนี้

๔.๖.๓.๑ แนวปฏิบัติและมาตรฐานข้อมูลเกี่ยวกับการประเมินความเสี่ยงของข้อมูล

๔.๖.๓.๒ แนวปฏิบัติเกี่ยวกับการจัดทำแผนเตรียมความพร้อมกรณีเกิดเหตุฉุกเฉิน

๔.๖.๓.๓ แนวปฏิบัติกรณีเกิดเหตุฉุกเฉินที่มีความเสี่ยงต่อข้อมูล

๔.๖.๔ ขอบเขตการวัดและประเมินผลการดำเนินการ

ให้ส่วนงานของ กอ.รมน. ที่มีฐานะเป็นเจ้าของข้อมูล และส่วนงานบริหารจัดการข้อมูล (ศูนย์ดิจิทัลเพื่อความมั่นคง กอ.รมน.) และทีมบริกรข้อมูล กอ.รมน. กำหนดโครงสร้างบุคลากร รวมทั้งจัดทำมาตรฐานและแนวปฏิบัติด้านการวัดและประเมินผลการดำเนินการเพื่อธรรมาภิบาลข้อมูล ให้เป็นไปตามนโยบายและแนวปฏิบัติกลางที่เอกสารธรรมาภิบาลข้อมูลของ กอ.รมน. กำหนด ตามรูปที่ ๔.๖ และครอบคลุมขอบเขตงานที่เกี่ยวข้องทั้งระบบ โดยมีทีมบริกรข้อมูล กอ.รมน. สนับสนุนการปฏิบัติ ให้คำปรึกษา รวมทั้งร่วมปฏิบัติ โดยมีขอบเขตงานที่ต้องดำเนินการ รวม ๒ เรื่อง ดังนี้

รูปที่ ๔.๖ แนวปฏิบัติเกี่ยวกับการตรวจสอบ วัดผล และประเมิน

๔.๖.๔.๑ แนวปฏิบัติและมาตรฐานข้อมูลเกี่ยวกับการตรวจสอบ วัดผล และประเมินความพร้อมและการดำเนินการเกี่ยวกับการธรรมาภิบาลข้อมูลในความรับผิดชอบ

๔.๖.๔.๒ แนวปฏิบัติและมาตรฐานข้อมูลเกี่ยวกับการแก้ไขและป้องกัน (Corrective and Preventive Action : CPA)

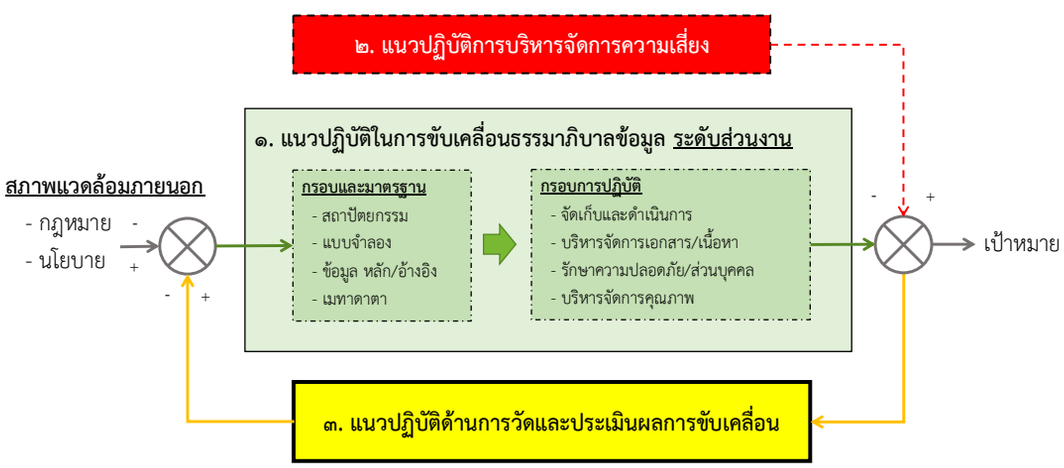
ในบทที่ ๔ นี้ ได้ชี้แจงรายละเอียดองค์ประกอบการธรรมาภิบาลข้อมูลระดับบริหาร โดยมีเป้าหมายเพื่อใช้สนับสนุนการปฏิบัติพันธกิจ ผ่านมุมมองวิสัยทัศน์ของ กอ.รมน. แล้วเชื่อมโยงไปถึงการกำหนดกรอบนโยบาย นิยามข้อมูล ซึ่งเป็นสิ่งจำเป็นต่อการกำหนดโครงสร้างบุคลากร รวมถึงมาตรฐานและแนวปฏิบัติในภาพรวม สำหรับรายละเอียดการปฏิบัติ จะกล่าวในบทที่ ๕ และบทที่ ๖ ต่อไป

บทที่ ๕
การธรรมาภิบาลข้อมูลของส่วนงานใน กอ.รมน.

๕.๑ กล่าวนำ

การธรรมาภิบาลข้อมูลของส่วนงานใน กอ.รมน. มีวัตถุประสงค์เพื่อขับเคลื่อนการบริหารจัดการข้อมูลของส่วนงานต่าง ๆ ภายใน กอ.รมน. ให้ดี มีคุณภาพ และปลอดภัย ภายใต้บทบาทและความรับผิดชอบที่กำหนดตามพระราชบัญญัติการรักษาความมั่นคงภายในราชอาณาจักร พ.ศ. ๒๕๕๑ โดยได้จัดทำให้อยู่ในรูปแบบแนวปฏิบัติ พร้อมรายละเอียดการดำเนินการในแต่ละองค์ประกอบการบริหารจัดการข้อมูลในแต่ละขั้นตอนบนวงจรชีวิตข้อมูลของ กอ.รมน. ได้แก่ ขั้นตอนสร้างและจัดเก็บ ใช้ เผยแพร่ จัดเก็บถาวร และทำลาย เพื่อให้ผู้ที่มีส่วนได้ส่วนเสีย มีความตระหนักรู้ เข้าใจ และสามารถนำไปใช้ยึดถือและขยายผลการปฏิบัติได้อย่างมั่นใจเชื่อมั่น อย่างต่อเนื่อง

ทั้งนี้ เพื่อให้เกิดความชัดเจน ได้จัดกลุ่มแนวปฏิบัติ แบ่งออกเป็น ๓ ด้าน ตามรูปที่ ๕.๑ ประกอบด้วย



รูปที่ ๕.๑ กรอบงานธรรมาภิบาลข้อมูลของส่วนงานใน กอ.รมน.

๕.๑.๑ แนวปฏิบัติในการขับเคลื่อนธรรมาภิบาลข้อมูลระดับส่วนงานใน กอ.รมน. : เป็นแนวปฏิบัติในยามปกติ เพื่อให้เกิดธรรมาภิบาลข้อมูล ผ่านกระบวนการเตรียมการ การบริหารจัดการ และการนำไปสู่การปฏิบัติที่เป็นรูปธรรม

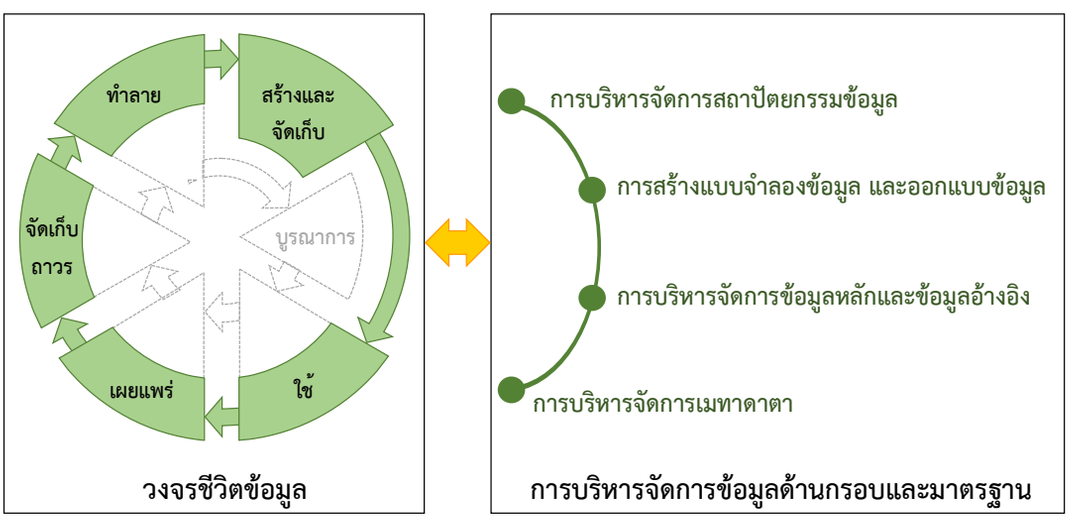
๕.๑.๒ แนวปฏิบัติการบริหารจัดการความเสี่ยง : เป็นแนวปฏิบัติเพื่อให้เกิดธรรมาภิบาลข้อมูลในยามที่เกิดเหตุผิดปกติ ฉุกเฉิน โดยให้ความสำคัญกับเหตุการณ์กรณีเกิดการรั่วไหลของข้อมูล และส่งผลกระทบร้ายแรงต่อความมั่นคงของประเทศ ความรับผิดชอบทางด้านกฎหมาย รวมถึงความเชื่อมั่นต่อ กอ.รมน. และระบบธรรมาภิบาลข้อมูลของ กอ.รมน.

๕.๑.๓ แนวปฏิบัติด้านการวัดและประเมินผลการขับเคลื่อนการดำเนินการ : เป็นแนวปฏิบัติเพื่อการตรวจสอบวัดผล ทั้งในด้านคุณภาพและประสิทธิภาพของการธรรมาภิบาลข้อมูลของ กอ.รมน. อย่างเป็นภาพรวม อันเป็นหนึ่งในกระบวนการของวงจรเดมมิ่ง (Deming Cycle) ที่กล่าวในบทที่ ๓ โดยนำไปประเมิน เปรียบเทียบกับวัตถุประสงค์ เป้าหมาย มาตรฐาน และแนวปฏิบัติ ที่ได้กำหนดขึ้นในห้วงต้นของก่อนการดำเนินการ เพื่อนำไปสู่การปรับปรุงแก้ไขอย่างเป็นระบบต่อเนื่องต่อไป

๕.๒ แนวปฏิบัติในการขับเคลื่อนธรรมาภิบาลข้อมูลของส่วนงานใน กอ.รมน.

๕.๒.๑ การกำหนดกรอบและมาตรฐาน

การกำหนดกรอบและมาตรฐาน เป็นการดำเนินการภายใต้องค์ประกอบการบริหารจัดการข้อมูลด้านการบริหารจัดการสถาปัตยกรรมข้อมูล การสร้างแบบจำลองและออกแบบข้อมูล การบริหารจัดการข้อมูลหลักและข้อมูลอ้างอิง การบริหารจัดการความมั่นคงปลอดภัยและการรักษาความเป็นส่วนบุคคลของข้อมูลและการบริหารจัดการเมทาดาตา ตามรูปที่ ๕.๒ โดยให้ส่วนงานเจ้าของข้อมูล ตรวจสอบแนวทางที่คณะกรรมการธรรมาภิบาลข้อมูล กอ.รมน. ได้ให้ความเห็นชอบความต้องการใช้งานข้อมูล และสภาพแวดล้อมที่เกี่ยวข้องกับข้อมูลทั้งหมด (ทั้งที่เป็นข้อมูลแบบมีโครงสร้าง แบบกึ่งโครงสร้าง และแบบไม่มีโครงสร้าง) และสรุปจัดทำเป็นแผนผัง แบบจำลองชุดข้อมูล พร้อมคำอธิบาย เพื่อให้ผู้ที่มีส่วนได้ส่วนเสีย เข้าใจและสามารถนำไปใช้ขยายผลในการดำเนินการต่อข้อมูลต่อไป ทั้งนี้ มีประเด็นที่ส่วนงานเจ้าของข้อมูล ต้องดำเนินการ สรุปได้ดังนี้



รูปที่ ๕.๒ การกำหนดกรอบและมาตรฐานธรรมาภิบาลบนวงจรชีวิตข้อมูล

๕.๒.๑.๑ ผู้ที่มีส่วนได้ส่วนเสียในกระบวนการ มีจำนวน ๕ กลุ่ม ประกอบด้วย : (๑) ส่วนงานเจ้าของข้อมูล (๒) ทีมบริหารจัดการข้อมูล (๓) ส่วนงานภายนอกอื่น ๆ (๔) ผู้ใช้งานข้อมูล และ (๕) เจ้าของข้อมูลส่วนบุคคล

๕.๒.๑.๒ จัดทำแบบจำลองสำหรับการออกแบบข้อมูล ในรูปไดอะแกรม (Diagram) หรือตารางข้อมูล ตามอนุผนวก ๑ การจัดทำแบบจำลองสำหรับการออกแบบข้อมูล (ISOC-DG-301) ประกอบผนวก ง

๕.๒.๑.๓ จัดทำมาตรฐานข้อมูล โดยกำหนดข้อมูลหลักและข้อมูลอ้างอิงที่ใช้ภายในส่วนงานทั้งหมด ตามอนุผนวก ๒ การจัดทำมาตรฐานข้อมูล (ISOC-DG-302) ประกอบผนวก ง

๕.๒.๑.๔ ประเมินความเสี่ยง และกำหนดระดับความเสี่ยงและระดับชั้นความลับของข้อมูล ให้มีความชัดเจน โดยใช้แบบฟอร์ม ตามอนุผนวก ๑ การประเมินความเสี่ยงของข้อมูล (ISOC-DG-201) ประกอบผนวก ค

๕.๒.๑.๕ จัดทำเมทาดาตา หรือคำอธิบายข้อมูลหลัก และกลุ่มข้อมูลอื่น ๆ (ถ้ามี) โดยใช้แบบฟอร์ม ตามอนุผนวก ๒ แบบฟอร์มเมทาดาตา (ISOC-DG-202) ประกอบผนวก ค

๕.๒.๑.๖ จัดทำสถาปัตยกรรมข้อมูล ที่ระบุวัตถุประสงค์ เป้าหมาย และตัวชี้วัดเกี่ยวกับข้อมูล โครงสร้างหมวดหมู่ ประเภท ระดับชั้นความลับ และการเชื่อมโยงแลกเปลี่ยนข้อมูล รวมทั้งแผนผังภาพรวม แสดงความสัมพันธ์ การเชื่อมโยงและการไหลของข้อมูลที่ส่วนงานต้องมีหรือควรมีใช้สนับสนุนการปฏิบัติภารกิจ ที่เป็นปัจจุบัน และรวมถึงแผนความต้องการใช้งานข้อมูลในอนาคต ตามอนุผนวก ๓ การจัดทำสถาปัตยกรรมข้อมูล (ISOC-DG-303) ประกอบผนวก ง

๕.๒.๑.๗ จัดทำระเบียบ ข้อตกลง มาตรฐาน เป้าหมาย และตัวชี้วัดการสร้างข้อมูล รวมทั้ง การเชื่อมโยงแลกเปลี่ยน จัดเก็บ จัดเก็บถาวร โอนย้าย เผยแพร่ ใช้ ประมวลผล หรือดำเนินการใด ๆ ต่อข้อมูล ภายในส่วนงาน ระหว่างส่วนงาน หรือบุคคลที่เกี่ยวข้อง ให้มีความชัดเจนและปลอดภัย ตามอนุผนวก ๑ การสร้าง จัดเก็บ และจัดเก็บถาวร (ISOC-DG-101) ประกอบผนวก ข

๕.๒.๑.๘ จัดทำระเบียบ ข้อปฏิบัติ มาตรฐาน เป้าหมาย และตัวชี้วัดด้านการรักษาความปลอดภัย เกี่ยวกับข้อมูล ในทุกขั้นตอน ตามระดับความเสี่ยงและระดับชั้นความลับ อย่างเหมาะสม ตามอนุผนวก ๒ การรักษาความปลอดภัยเกี่ยวกับข้อมูล (ISOC-DG-102) ประกอบผนวก ข

๕.๒.๑.๙ จัดทำระเบียบ ข้อปฏิบัติ มาตรฐาน เป้าหมาย และตัวชี้วัดด้านการคุ้มครองข้อมูล ส่วนบุคคล ในทุกขั้นตอนของวงจรชีวิตข้อมูล ได้แก่ การสร้างและจัดเก็บ ใช้ เผยแพร่ จัดเก็บถาวร และทำลาย หรือการดำเนินการใด ๆ ต่อข้อมูลส่วนบุคคล โดยต้องเป็นไปตามข้อตกลง หรือกระบวนการยินยอมของเจ้าของข้อมูล ส่วนบุคคล และต้องไม่ฝ่าฝืนหรือขัดต่อระเบียบ กฎหมาย และแนวทางที่ผู้ควบคุมข้อมูลส่วนบุคคลกำหนด อีกทั้งต้องสามารถป้องกันการสูญหาย ถูกทำลาย ถูกปลอมแปลง ถูกเปิดเผยหรือถูกเข้าถึงจากผู้ไม่ได้รับอนุญาต หรือทำให้ข้อมูลสามารถระบุถึงตัวบุคคลได้ ตามอนุผนวก ๓ การคุ้มครองข้อมูลส่วนบุคคล (ISOC-DG-103) ประกอบผนวก ข

๕.๒.๑.๑๐ จัดทำระเบียบ ข้อปฏิบัติ มาตรฐาน เป้าหมาย และตัวชี้วัดด้านคุณภาพข้อมูล ทั้งระบบ ตั้งแต่การกำหนดเป้าหมาย การประเมิน การวิเคราะห์ การวางแผน การปรับปรุง และการควบคุม คุณภาพข้อมูล เพื่อให้มีความถูกต้อง ครบถ้วน สอดคล้องต้องกัน เป็นปัจจุบัน ตรงความต้องการใช้งาน และมีความพร้อมใช้งาน ตามอนุผนวก ๔ การควบคุมคุณภาพข้อมูล (ISOC-DG-104) ประกอบผนวก ข

๕.๒.๑.๑๑ แต่งตั้งทีมบริหารจัดการข้อมูลหรือเจ้าหน้าที่บริหารจัดการข้อมูล ให้มีหน้าที่และอำนาจ ดังต่อไปนี้

๕.๒.๑.๑๑ (๑) สร้าง จัดเก็บ เชื่อมโยงแลกเปลี่ยน ใช้ สำรองและกู้คืน จัดเก็บถาวร เผยแพร่ และทำลายข้อมูลที่อยู่ในความรับผิดชอบ

๕.๒.๑.๑๑ (๒) ควบคุมการดำเนินการเกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล รวมทั้งกำกับดูแลการรักษาความปลอดภัย การจัดเก็บ ป้องกันการสูญหาย เข้าถึง ใช้ เปลี่ยนแปลง แก้ไข แลกเปลี่ยน โอนย้าย หรือทำลายข้อมูลส่วนบุคคล ให้เป็นไปตามระเบียบ กฎหมาย และแนวทางที่ผู้ควบคุมข้อมูลส่วนบุคคลกำหนด โดยบันทึกรายการเพื่อให้เจ้าของข้อมูลส่วนบุคคลและส่วนงานที่เกี่ยวข้อง สามารถตรวจสอบได้

๕.๒.๑.๑๒ ติดตาม ตรวจสอบสภาพแวดล้อมการดำเนินการ รวมถึงความต้องการใช้งาน (เพิ่มเติม) รวมทั้งกำกับดูแลการใช้งานข้อมูล อย่างต่อเนื่อง อีกทั้งกำหนดให้ทบทวน ปรับปรุงความถูกต้องและความทันสมัยในข้อ ๕.๒.๑.๒ – ๕.๒.๑.๑๑ ให้มีความเหมาะสม ในทันทีที่มีการเปลี่ยนแปลง หรืออย่างน้อย ปีละ ๑ ครั้ง ดังนี้

๕.๒.๑.๑๒ (๑) บันทึกผลการตรวจสอบการปฏิบัติด้านข้อมูล โดยใช้แบบฟอร์มตามอนุผนวก ๓ การตรวจสอบการปฏิบัติด้านข้อมูล (ISOC-DG-203) ประกอบผนวก ค

๕.๒.๑.๑๒ (๒) บันทึกผลการตรวจสอบการรักษาความมั่นคงปลอดภัย โดยใช้แบบฟอร์มตามอนุผนวก ๔ การตรวจสอบการรักษาความมั่นคงปลอดภัย (ISOC-DG-204) ประกอบผนวก ค

๕.๒.๑.๑๒ (๓) บันทึกผลการตรวจสอบการคุ้มครองข้อมูลส่วนบุคคล โดยใช้แบบฟอร์มตามอนุผนวก ๕ การตรวจสอบการคุ้มครองข้อมูลส่วนบุคคล (ISOC-DG-205) ประกอบผนวก ค

๕.๒.๑.๑๒ (๔) บันทึกผลการตรวจสอบการรักษาความปลอดภัยของระบบและเครือข่าย โดยใช้แบบฟอร์ม ตามอนุผนวก ๖ การตรวจสอบการรักษาความปลอดภัยของระบบและเครือข่าย (ISOC-DG-206) ประกอบผนวก ค

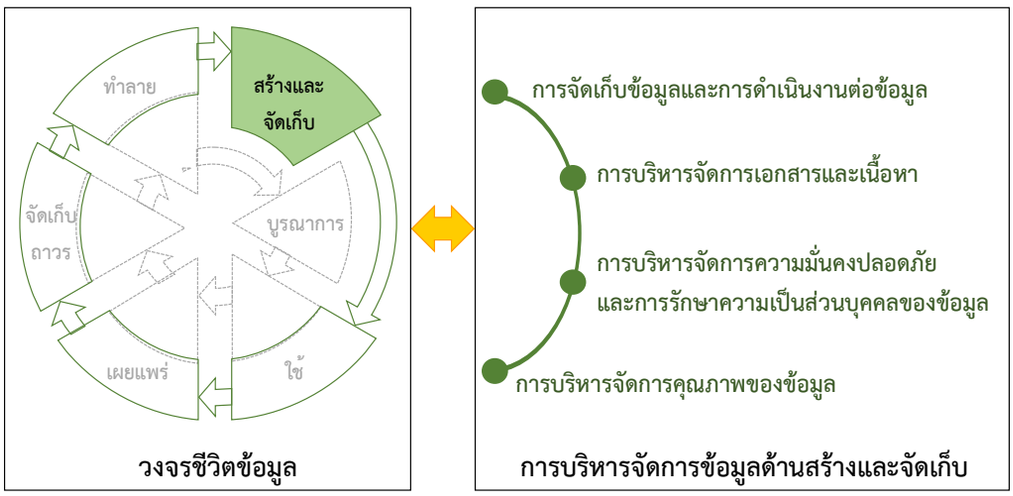
๕.๒.๒ การกำหนดกรอบการปฏิบัติ

ธรรมาภิบาลในวงจรชีวิตข้อมูลที่เกี่ยวข้องกับการนำไปสู่การปฏิบัติงานในกรอบหน้าที่และอำนาจของ กอ.รมน. มีรวม ๕ ขั้นตอน ดังนี้

๕.๒.๒.๑ ขั้นตอนสร้างและจัดเก็บ

ในขั้นตอนสร้างและจัดเก็บ มีผู้ที่มีส่วนได้ส่วนเสีย และแนวปฏิบัติในแต่ละประเด็นขององค์ประกอบการบริหารจัดการข้อมูลด้านความมั่นคงที่เกี่ยวข้อง ได้แก่ การจัดเก็บและการดำเนินงานต่อข้อมูลที่มีโครงสร้าง การบริหารจัดการเอกสารและเนื้อหาข้อมูลแบบกึ่งโครงสร้างและแบบไม่มีโครงสร้าง การบริหารจัดการความมั่นคงปลอดภัยและการรักษาความเป็นส่วนบุคคลของข้อมูล และการบริหารจัดการคุณภาพของข้อมูล ตามรูปที่ ๕.๓ ดังนี้

๕.๒.๒.๑ (๑) ผู้ที่มีส่วนได้ส่วนเสียในขั้นตอนสร้างและจัดเก็บ มีจำนวน ๖ กลุ่ม ประกอบด้วย : (๑) ส่วนงานเจ้าของข้อมูล (๒) ทีมบริหารจัดการข้อมูล (๓) ผู้สร้างข้อมูล (๔) เจ้าของข้อมูลส่วนบุคคล (๕) ทีมบริกรข้อมูล กอ.รมน. และ (๖) เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล



รูปที่ ๕.๓ ความสัมพันธ์การบริหารจัดการข้อมูลด้านสร้างและจัดเก็บ

๕.๒.๒.๑ (๒) ให้ส่วนงานเจ้าของข้อมูล กำหนดวิธีการดำเนินการ เครื่องมือ และสภาพแวดล้อม สำหรับการสร้างและจัดเก็บ รวมทั้งการบันทึกประวัติข้อมูล ให้มีความชัดเจน ปลอดภัย และเหมาะสมสอดคล้องกับผลประเมินระดับความเสี่ยงของข้อมูล รวมทั้งควบคุมคุณภาพของข้อมูล ให้เป็นไปตามเป้าหมาย แนวทาง ข้อปฏิบัติ ข้อกำหนด และมาตรฐานข้อมูลในข้อ ๕.๒.๑.๗ – ๕.๒.๑.๑๐ เช่น การจัดเก็บและรักษาข้อมูลที่มีความเสี่ยง ข้อมูลที่มีระดับชั้นความลับ และข้อมูลส่วนบุคคล ให้ทำการเข้ารหัสข้อมูลตามระดับความเสี่ยงของข้อมูลแต่ละประเภทด้วย เป็นต้น

๕.๒.๒.๑ (๓) ให้ส่วนงานเจ้าของข้อมูล กำหนดวิธีการดำเนินการ เครื่องมือ และสภาพแวดล้อมกรณีมีหน่วยงานภายนอก ร้องขอเชื่อมโยง แลกเปลี่ยน โอนย้ายข้อมูล โดยต้องขอนำเรียนอนุมัติผู้บริหารระดับสูง (CEO) และต้องจัดทำเป็นข้อตกลงการใช้งานข้อมูลระหว่างส่วนงานที่เกี่ยวข้อง โดยระบุวัตถุประสงค์ และรายละเอียดการขอใช้ข้อมูล ให้มีความชัดเจน ทั้งนี้หากเป็นการแลกเปลี่ยนและเชื่อมโยงข้อมูลที่มีระดับชั้นความลับ หรือข้อมูลส่วนบุคคล จะต้องปฏิบัติตามมาตรการที่เกี่ยวข้อง อย่างเคร่งครัด

๕.๒.๒.๑ (๔) ให้ส่วนงานเจ้าของข้อมูล กำหนดห้วงระยะเวลาและดำเนินการจัดเก็บข้อมูล ตามแนวทางหรือมาตรฐานที่คณะกรรมการธรรมาภิบาลข้อมูล กอ.รมน. เห็นชอบ พร้อมทั้งบันทึกลงในบัญชีคุมข้อมูล ตามเงื่อนไข ดังนี้

๕.๒.๒.๑ (๔.๑) ระยะเวลาในการจัดเก็บจะต้องอยู่ภายใต้กรอบกฎหมาย ระเบียบข้อบังคับ หรือข้อตกลงระหว่างผู้ที่มีส่วนได้ส่วนเสียเกี่ยวกับการใช้ข้อมูล

๕.๒.๒.๑ (๔.๒) ระยะเวลาในการจัดเก็บจะต้องไม่นานเกินกว่าความจำเป็นตามลักษณะข้อมูล

๕.๒.๒.๑ (๕) ให้ส่วนงานเจ้าของข้อมูล กำหนดวิธีการดำเนินการ เครื่องมือ และสภาพแวดล้อม สำหรับการสำรองและกู้คืน ดังนี้

๕.๒.๒.๑ (๕.๑) กำหนดวิธีการหรือระบบ ขั้นตอน ช่วงเวลา สำหรับการสำรองและกู้คืนข้อมูล ทั้งนี้ให้ทดสอบวิธีการหรือระบบ ขั้นตอน สำหรับสำรองและกู้คืนข้อมูล อย่างน้อยปีละ ๑ ครั้ง รวมทั้งก่อนการนำข้อมูลที่ได้สำรองหรือกู้คืน ต้องตรวจสอบความถูกต้องครบถ้วนสมบูรณ์ของข้อมูลก่อนทุกครั้ง

๕.๒.๒.๑ (๕.๒) จัดทำบันทึกประวัติการสำรองหรือกู้คืนข้อมูล โดยระบุรายละเอียด ได้แก่ เวลาเริ่มต้นและสิ้นสุดในการดำเนินการ ชื่อเจ้าหน้าที่ผู้ดำเนินการ ประเภทและชั้นความลับของข้อมูล และรายละเอียดอื่น ๆ (เช่น ในกรณีที่เกิดข้อผิดพลาดในการสำรองหรือกู้คืนข้อมูล และวิธีดำเนินการแก้ไขข้อผิดพลาด เป็นต้น) ตามอนุผนวก ๗ การบันทึกประวัติการสำรองหรือกู้คืนข้อมูล (ISOC-DG-207) ประกอบผนวก ค

๕.๒.๒.๑ (๕.๓) หากมีความจำเป็นต้องทำการกู้คืนข้อมูลให้ตรวจสอบคุณภาพข้อมูล และใช้ข้อมูลที่ทันสมัยที่สุด (Latest Update) ที่ได้สำรองไว้ หรือข้อมูลที่เหมาะสมที่สุด ทั้งนี้ต้องแจ้งความคืบหน้าการดำเนินการ ให้ผู้ใช้งานข้อมูลและผู้ที่มีส่วนได้ส่วนเสีย ทราบอย่างต่อเนื่อง จนกว่าจะทำการกู้คืนข้อมูลจะเสร็จสิ้นอย่างสมบูรณ์

๕.๒.๒.๑ (๖) ให้ส่วนงานเจ้าของข้อมูล จัดทำบัญชีควบคุมข้อมูล และเก็บรักษาพร้อมรับการตรวจจากทีมบริกรข้อมูล กอ.รมน. และเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล เมื่อได้รับการประสาน ดังนี้

๕.๒.๒.๑ (๖.๑) บัญชีควบคุมการสร้างข้อมูล บันทึกและเก็บรักษารายการข้อมูลที่ไม่มีชั้นความลับ โดยใช้แบบฟอร์ม ตามอนุผนวก ๘ บัญชีคุมข้อมูลปกติ (ISOC-DG-208) ประกอบผนวก ค

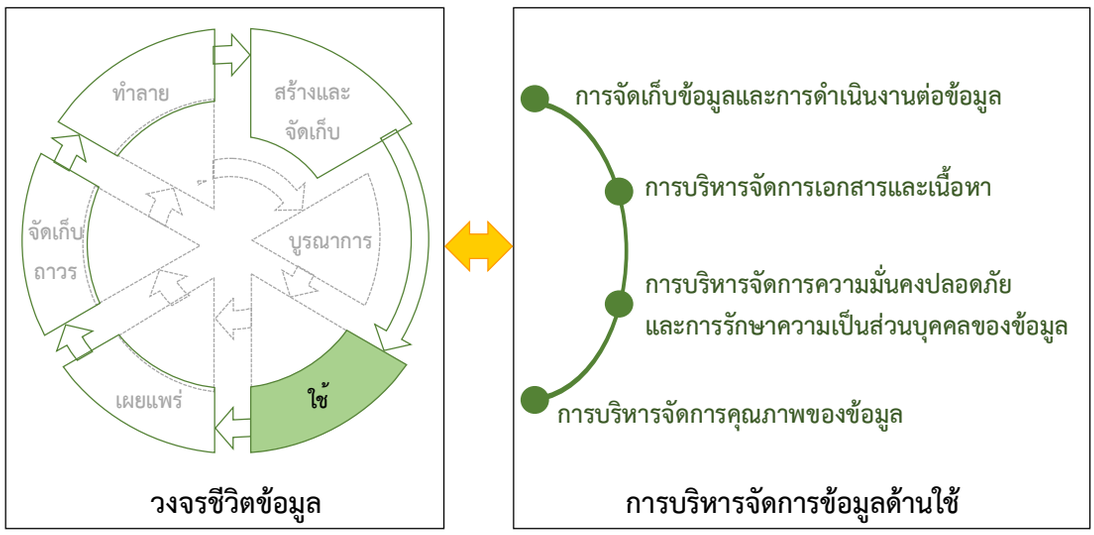
๕.๒.๒.๑ (๖.๒) บัญชีควบคุมรายการชุดข้อมูลที่มีชั้นความลับและต้องการดูแลเป็นกรณีพิเศษ โดยใช้แบบฟอร์ม ตามอนุผนวก ๙ บัญชีคุมข้อมูลพิเศษ (ISOC-DG-209) ประกอบผนวก ค

๕.๒.๒.๑ (๖.๓) บัญชีควบคุมการขอความยินยอมในการเปิดเผยข้อมูลของเจ้าข้อมูลส่วนบุคคล โดยใช้แบบฟอร์ม ตามอนุผนวก ๑๐ การขอความยินยอมให้ข้อมูล (ISOC-DG-210) ประกอบผนวก ค

๕.๒.๒.๑ (๗) ให้ผู้สร้างข้อมูล ทีมบริหารจัดการข้อมูล ปฏิบัติตามวิธีการ เครื่องมือและสภาพแวดล้อมสำหรับการสร้าง จัดเก็บ และเชื่อมโยงแลกเปลี่ยนข้อมูล ตามที่ส่วนงานเจ้าของข้อมูลกำหนด สำหรับกรณีการรวบรวมข้อมูลส่วนบุคคล ให้ดำเนินการและควบคุมการดำเนินการ โดยต้องแจ้งวัตถุประสงค์ ระยะเวลาในการเก็บรวบรวม ประเภทของบุคคลหรือส่วนงานที่อาจเข้าถึงหรือเปิดเผย สิทธิของเจ้าของข้อมูลส่วนบุคคลตามกฎหมายที่เกี่ยวข้อง และรวมถึงข้อมูลเกี่ยวกับผู้ควบคุมข้อมูลส่วนบุคคล เพื่อให้เจ้าของข้อมูลส่วนบุคคลยินยอมก่อนหรือในขณะเก็บรวบรวมข้อมูลส่วนบุคคล

๕.๒.๒.๒ ขั้นตอนใช้

ในขั้นตอนใช้ มีผู้ที่มีส่วนได้ส่วนเสีย และแนวปฏิบัติในแต่ละประเด็นขององค์ประกอบการบริหารจัดการข้อมูลด้านความมั่นคงที่เกี่ยวข้อง ได้แก่ การจัดเก็บและการดำเนินงานต่อข้อมูล การบริหารจัดการเอกสารและเนื้อหาข้อมูล การบริหารจัดการความมั่นคงปลอดภัยและการรักษาความเป็นส่วนบุคคลของข้อมูล และการบริหารจัดการคุณภาพของข้อมูล ตามรูปที่ ๕.๔ ดังนี้



รูปที่ ๕.๔ ความสัมพันธ์การบริหารจัดการข้อมูลด้านใช้

๕.๒.๒.๒ (๑) ผู้ที่มีส่วนได้ส่วนเสียในขั้นตอนใช้ มีจำนวน ๖ กลุ่ม ประกอบด้วย : (๑) ส่วนงานเจ้าของข้อมูล (๒) ทีมบริหารจัดการข้อมูล (๓) ผู้ใช้งานข้อมูล (๔) ทีมบริกรข้อมูล กอ.รมน. (๕) เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล และ (๖) ศูนย์ดิจิทัลเพื่อความมั่นคง กอ.รมน.

๕.๒.๒.๒ (๒) ให้ส่วนงานเจ้าของข้อมูล จัดทำข้อตกลงหรือข้อตกลงร่วม เกี่ยวกับการใช้งานข้อมูลในทุกขั้นตอนการปฏิบัติ ทั้งที่เป็นข้อมูลหลัก ข้อมูลอ้างอิง หรือกลุ่มข้อมูลอื่น ๆ ของส่วนงานหรือระหว่างส่วนงาน ตามอนุผนวก ๔ การควบคุมคุณภาพข้อมูล (ISOC-DG-104) ประกอบผนวก ข ในประเด็นดังต่อไปนี้

๕.๒.๒.๒ (๒.๑) หัวข้อเรื่อง/ประเด็น ลักษณะและวัตถุประสงค์ในการใช้ข้อมูล ระยะเวลาในการใช้ และคำอธิบาย

๕.๒.๒.๒ (๒.๒) ประเภทของข้อมูล และเจ้าของข้อมูล โดยให้ระบุถึงความอ่อนไหวของข้อมูล ข้อมูลที่มีระดับชั้นความลับ ข้อมูลส่วนบุคคล หรือข้อมูลที่ส่งผลกระทบต่อความมั่นคงของชาติ

๕.๒.๒.๒ (๒.๓) ข้อกำหนดและสิทธิ ทั้งในระดับผู้ใช้งานข้อมูลและส่วนงานเจ้าของข้อมูล (กรณีเป็นข้อมูลของส่วนงานภายนอก)

๕.๒.๒.๒ (๒.๔) รายละเอียดเกี่ยวกับขอบเขตการใช้ของผู้ใช้งานข้อมูล รวมถึงการประมวลผล การรักษาความปลอดภัยข้อมูล การรักษาความลับ และการยินยอมให้ผู้ควบคุมข้อมูลส่วนบุคคล ตรวจสอบการใช้งานข้อมูล

๕.๒.๒.๒ (๓) ให้ส่วนงานเจ้าของข้อมูล ควบคุมกำกับดูแลความปลอดภัยและความเหมาะสมในการใช้งานข้อมูล และข้อมูลส่วนบุคคล โดยกำหนดมาตรการควบคุม ดังนี้

๕.๒.๒.๒ (๓.๑) กำหนดรายละเอียดข้อมูล เพื่อให้ผู้ใช้งานข้อมูลรับทราบถึงระดับในการรักษาความปลอดภัยที่เหมาะสม ตามสถานการณ์ และระดับผลประเมินความเสี่ยง

๕.๒.๒.๒ (๓.๒) กำหนดมาตรการและกำกับดูแลการรักษาความปลอดภัยและความเหมาะสมในการใช้งานข้อมูล ซึ่งรวมถึงการเชื่อมโยงและการประมวลผลข้อมูลด้วย

๕.๒.๒.๒ (๓.๓) ตรวจสอบร่วมกับศูนย์ดิจิทัลเพื่อความมั่นคง กอ.รมน. กรณีผู้ใช้งานข้อมูลมีความประสงค์ใช้งานอุปกรณ์เคลื่อนที่หรืออุปกรณ์ส่วนตัว ก่อนการอนุมัติการเข้าใช้งาน

๕.๒.๒.๒ (๓.๔) รักษาความปลอดภัยระหว่างการใช้งานข้อมูลให้เหมาะสมเพียงพอต่อระดับความเสี่ยงของข้อมูล และตลอดเวลาที่มีการใช้งานข้อมูล

๕.๒.๒.๒ (๓.๕) ควรมีระบบบริหารจัดการทรัพย์สินข้อมูลเพื่อควบคุมตรวจสอบการส่งคืน หรือทำลายทรัพย์สินข้อมูล โดยเฉพาะข้อมูลที่มีความเสี่ยงสูง อย่างเป็นระบบ

๕.๒.๒.๒ (๓.๖) จัดทำเอกสารควบคุมการเข้าถึงข้อมูล รวมทั้งกำกับดูแลการเข้าถึงข้อมูล ตามอนุผนวก ๔ การจัดทำเอกสารควบคุมการเข้าถึงข้อมูล (ISOC-DG-304) ประกอบผนวก ง

๕.๒.๒.๒ (๔) ให้ส่วนงานเจ้าของข้อมูล กำหนดมาตรการและควบคุมการรักษาความปลอดภัยเพิ่มเติม กรณีข้อมูลที่มีความอ่อนไหว ข้อมูลที่ส่งผลกระทบต่อความมั่นคงของชาติ ข้อมูลที่อาจส่งผลกระทบต่อสิทธิและเสรีภาพของบุคคล หรือข้อมูลความลับทางราชการ ดังนี้

๕.๒.๒.๒ (๔.๑) ประสานศูนย์ดิจิทัลเพื่อความมั่นคง กอ.รมน. ร่วมตรวจสอบและประเมินสภาพแวดล้อมการรักษาความปลอดภัยของระบบเครือข่ายคอมพิวเตอร์ของผู้ใช้งานข้อมูล รวมทั้งในกรณีที่มีความประสงค์ใช้งานอุปกรณ์เคลื่อนที่หรืออุปกรณ์ส่วนตัว เพื่อขออนุมัติตามสายงานด้านการข่าว กอ.รมน. และนำผลไปใช้ประกอบในการพิจารณาให้สิทธิในการเข้าถึงข้อมูล

๕.๒.๒.๒ (๔.๒) ก่อนการอนุมัติสิทธิในการเข้าถึงข้อมูลให้กับผู้ใช้งานข้อมูล ต้องตรวจสอบรายละเอียดตามแนวทางหรือมาตรฐานที่คณะกรรมธรรมาภิบาลข้อมูล กอ.รมน. เห็นชอบ ทั้งนี้ต้องระงับสิทธิการเข้าถึงข้อมูลของผู้ใช้งาน เมื่อตรวจพบการไม่ปฏิบัติตามแนวทางหรือมาตรฐานที่กำหนด หรือมีเหตุอันควร ในทันที

๕.๒.๒.๒ (๔.๓) ให้เข้ารหัสข้อมูลตลอดระยะเวลาที่มีการใช้งานหรือดำเนินการใด ๆ กับข้อมูล โดยตรวจสอบการดำเนินการตามมาตรการการเข้ารหัสข้อมูลที่กำหนด ตามแนวทางหรือมาตรฐานที่คณะกรรมธรรมาภิบาลข้อมูล กอ.รมน. เห็นชอบ

๕.๒.๒.๒ (๔.๔) ทั้งนี้ ส่วนงานเจ้าของข้อมูล และผู้ใช้ข้อมูลต้องพร้อมรับการตรวจสอบการใช้ข้อมูลดังกล่าวจากทีมบริกรข้อมูล กอ.รมน. และเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล เมื่อได้รับการประสาน

๕.๒.๒.๒ (๕) ให้ผู้ใช้งานข้อมูล และทีมบริหารจัดการข้อมูล เลือกใช้งานข้อมูลที่มีคุณภาพ ถูกต้อง ครบถ้วน สอดคล้องต้องกัน เป็นปัจจุบัน และตรงตามความต้องการหรือวัตถุประสงค์การดำเนินการที่แท้จริง โดยเข้าใช้งานข้อมูลตามวิธีการ เครื่องมือ และสภาพแวดล้อมการเข้าใช้งานข้อมูลตามที่ส่วนงานเจ้าของข้อมูลกำหนด โดยบันทึกประวัติการเข้าใช้งานข้อมูล โดยใช้แบบฟอร์ม ตามอนุผนวก ๑๑ การบันทึกประวัติการเข้าใช้งานข้อมูล (ISOC-DG-211) ประกอบผนวก ค ดังนี้

๕.๒.๒.๒ (๕.๑) ชุดข้อมูลที่ใช้งาน และรายละเอียดที่บ่งบอกถึงการอนุญาตให้ผู้ใช้งานข้อมูลสามารถเข้าถึงชุดข้อมูลได้ เช่น เอกสารคำขอ หรือข้อตกลงฯ ที่กำหนดให้เข้าถึงชุดข้อมูล

๕.๒.๒.๒ (๕.๒) รายละเอียดผู้ใช้งานข้อมูล เช่น บัญชีผู้ใช้งาน

๕.๒.๒.๒ (๕.๓) วันเวลาที่ใช้งานข้อมูล รวมถึงรายละเอียดการใช้งานข้อมูล เป็นต้น

๕.๒.๒.๒ (๖) ให้ส่วนงานเจ้าของข้อมูล ควบคุมและตรวจสอบการดำเนินการของผู้ใช้งานข้อมูล รวมทั้งตรวจสอบบันทึกประวัติการใช้งานข้อมูล ตามวงรอบภายในระยะเวลาที่เหมาะสมกับระดับความเสี่ยงของข้อมูล เพื่อเป็นมาตรการควบคุมในการรักษาความปลอดภัย และตรวจสอบควบคุมการเข้าถึงข้อมูลโดยจัดเก็บเป็นหลักฐานในการประเมินผล ตามอนุผนวก ๑๒ การบันทึกการตรวจสอบประวัติการเข้าใช้งานข้อมูล (ISOC-DG-212) ประกอบผนวก ค ดังนี้

๕.๒.๒.๒ (๖.๑) วัน เวลาในการประเมิน ผู้ประเมิน ผู้รับการประเมิน และประเภทของข้อมูลที่มีการนำไปใช้งาน

๕.๒.๒.๒ (๖.๒) ข้อมูลนโยบายด้านการรักษาความปลอดภัยข้อมูลของผู้รับการประเมิน หรือใบรับรองมาตรฐานด้านการรักษาความปลอดภัย

๕.๒.๒.๒ (๖.๓) ข้อมูล และรายละเอียดข้อมูล ได้แก่ ปริมาณ ประเภทและคุณภาพ ที่ดำเนินการโดยผู้ใช้งานข้อมูล รวมทั้งเหตุผลในการใช้งาน

๕.๒.๒.๒ (๖.๔) ตรวจสอบการควบคุมด้านการรักษาความปลอดภัยข้อมูล ที่เหมาะสมเพียงพอต่อระดับความเสี่ยงของข้อมูล

๕.๒.๒.๒ (๖.๕) ตรวจสอบการแบ่งปันข้อมูล หรือการให้บุคคลที่สามดำเนินการต่อข้อมูล (ถ้ามี) ให้เป็นไปตามข้อตกลงในการใช้ข้อมูล

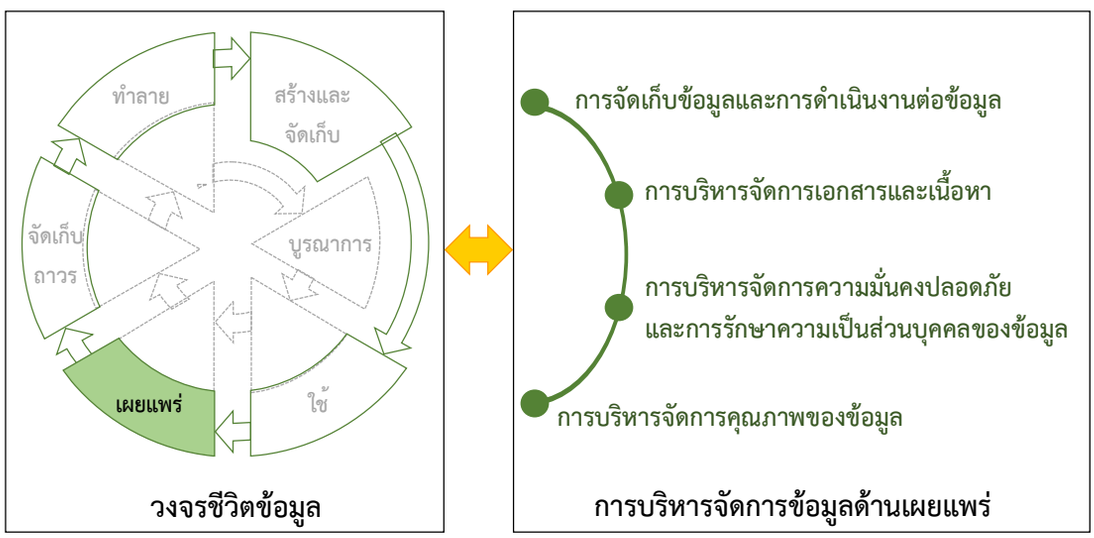
๕.๒.๒.๒ (๖.๖) ทั้งนี้ ให้จัดทำบันทึกประวัติ ข้อพิจารณา คำแนะนำเพิ่มเติม เพื่อนำไปใช้ประกอบการตรวจสอบครั้งต่อ ๆ ไปด้วย

๕.๒.๒.๒ (๗) ให้ส่วนงานเจ้าของข้อมูล ตรวจสอบสภาพแวดล้อมที่เกี่ยวกับการใช้งานข้อมูล เช่น การใช้เครือข่ายและอุปกรณ์ในการเข้าถึงข้อมูลของผู้ใช้งานข้อมูล ในทุกขั้นตอน ทั้งนี้หากตรวจพบการปฏิบัติที่ไม่เป็นไปตามข้อกำหนด ระเบียบ กฎหมาย หรือไม่ได้รับอนุญาต ให้ถือเป็นการละเมิดการรักษาความมั่นคงปลอดภัยข้อมูล และมีสิทธิในการระงับการเข้าถึงข้อมูลของผู้ใช้งานทันที และบันทึกในแบบฟอร์มตามอนุผนวก ๑๓ การบันทึกการระงับการเข้าถึงข้อมูล (ISOC-DG-213) ประกอบผนวก ค

๕.๒.๒.๒ (๘) ให้ส่วนงานเจ้าของข้อมูล สนับสนุนสถาปัตยกรรมข้อมูล แบบจำลองข้อมูล รวมทั้งเมทาดาตา ให้กับส่วนงาน หรือผู้ใช้ข้อมูล หรือผู้ที่เกี่ยวข้อง เพื่ออำนวยความสะดวกต่อการสืบค้นค้นหา และเข้าถึงข้อมูลได้โดยสะดวก

๕.๒.๒.๓ ขั้นตอนเผยแพร่

ในขั้นตอนเผยแพร่ มีผู้ที่มีส่วนได้ส่วนเสีย และแนวปฏิบัติในแต่ละประเด็นขององค์ประกอบการบริหารจัดการข้อมูลด้านความมั่นคงที่เกี่ยวข้อง ได้แก่ การจัดเก็บและการดำเนินงานต่อข้อมูล การบริหารจัดการเอกสารและเนื้อหาข้อมูล การบริหารจัดการความมั่นคงปลอดภัยและการรักษาความเป็นส่วนบุคคลของข้อมูล และการบริหารจัดการคุณภาพของข้อมูล ตามรูปที่ ๕.๕ ดังนี้



รูปที่ ๕.๕ ความสัมพันธ์การบริหารจัดการข้อมูลด้านเผยแพร่

๕.๒.๒.๓ (๑) ผู้ที่มีส่วนได้ส่วนเสียในขั้นตอนเผยแพร่ มีจำนวน ๖ กลุ่ม ประกอบด้วย : (๑) ส่วนงานเจ้าของข้อมูล (๒) ผู้ใช้งานข้อมูล (๓) ทีมบริหารจัดการข้อมูล (๔) ทีมบริกรข้อมูล กอ.รมน. (๕) เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล และ (๖) ศูนย์ดิจิทัลเพื่อความมั่นคง กอ.รมน.

๕.๒.๒.๓ (๒) ให้ส่วนงานเจ้าของข้อมูล วางแผน กำหนดแนวทาง บริหารจัดการตรวจสอบคุณภาพข้อมูล และดำเนินการเผยแพร่ข้อมูลที่อยู่ในความรับผิดชอบของส่วนงาน ตามแนวทางหรือมาตรฐานที่คณะกรรมการธรรมาภิบาลข้อมูล กอ.รมน. กำหนด โดยมีการรักษาความมั่นคงปลอดภัยและอำนวยความสะดวกในการเผยแพร่ และเปิดเผยข้อมูล อย่างเป็นระบบ ดังนี้

๕.๒.๒.๓ (๒.๑) สำรวจความต้องการ ตรวจสอบและคัดเลือกข้อมูลที่จะเผยแพร่ รวมทั้งตรวจสอบและปรับปรุงคุณภาพข้อมูล เพื่อจัดทำรายการบัญชีข้อมูลเผยแพร่ ที่ระบุประเภทชุดข้อมูล และแนวทางการเผยแพร่ โดยใช้แบบฟอร์ม ตามอนุผนวก ๑๔ รายการบัญชีข้อมูลเผยแพร่ (ISOC-DG-214) ประกอบผนวก ค

๕.๒.๒.๓ (๒.๒) ทวนสอบรายการบัญชีข้อมูลเผยแพร่ ต้องไม่มีชุดข้อมูลที่ขัดต่อกฎหมาย ระเบียบ ข้อบังคับ คำสั่ง นโยบาย แนวปฏิบัติ ความมั่นคงของชาติ ความลับทางราชการ หรือก้าวล่วงความเป็นส่วนตัวของบุคคล ทั้งนี้กรณีการเผยแพร่ข้อมูลส่วนบุคคล ต้องได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคล หรืออยู่ในขอบเขตที่กฎหมายกำหนด เท่านั้น

๕.๒.๒.๓ (๒.๓) เตรียมข้อมูลให้อยู่ในรูปแบบที่ง่ายต่อการเผยแพร่ และเป็นมาตรฐานสากล รวมทั้งเมทาดาตาของข้อมูล

๕.๒.๒.๓ (๒.๔) กำหนดมาตรการในการรักษาความปลอดภัยข้อมูล การเข้าถึง การแก้ไขเปลี่ยนแปลงข้อมูล เป้าหมายการเผยแพร่ข้อมูล และการป้องกันข้อมูลที่สามารถระบุตัวบุคคล ได้แก่ การพลางหรือปกปิดข้อมูลบางส่วนเพื่อจำกัดการเข้าถึงข้อมูลทั้งหมด หรือการทำข้อมูลนิรนาม

๕.๒.๒.๓ (๒.๕) กำหนดช่องทางเผยแพร่ชุดข้อมูล ผ่านระบบสื่อสารข้อมูลของ กอ.รมน. รวมทั้งหน่วยงานของรัฐ ที่มีการรักษาความมั่นคงปลอดภัยไซเบอร์ เป็นหลัก

๕.๒.๒.๓ (๓) ในกรณีเผยแพร่ข้อมูลภายใน กอ.รมน. หรือระหว่างหน่วยงาน ให้ส่วนงานเจ้าของข้อมูล จัดทำข้อตกลงร่วมเกี่ยวกับการเผยแพร่ข้อมูล ตามอนุผนวก ๕ ข้อตกลงร่วมเกี่ยวกับการเผยแพร่ข้อมูล (ISOC-DG-105) ประกอบผนวก ข ในประเด็นดังต่อไปนี้

๕.๒.๒.๓ (๓.๑) หัวข้อเรื่อง/ประเด็น ลักษณะและวัตถุประสงค์ในการเผยแพร่ ระยะเวลาในการเผยแพร่ และการทำลายข้อมูล และคำอธิบาย

๕.๒.๒.๓ (๓.๒) ประเภทของข้อมูล และเจ้าของข้อมูล โดยให้ตรวจสอบ และระบุถึงความอ่อนไหวของข้อมูล ข้อมูลที่มีระดับชั้นความลับ ข้อมูลส่วนบุคคล หรือข้อมูลที่ส่งผลกระทบต่อความมั่นคงของชาติ (ซึ่งควรหลีกเลี่ยงในการเผยแพร่)

๕.๒.๒.๓ (๓.๓) วิธีการ ข้อกำหนด สิทธิ รวมทั้งการอำนวยความสะดวกให้กับผู้ใช้งานข้อมูล

๕.๒.๒.๓ (๓.๔) รายละเอียดเกี่ยวกับขอบเขตการเข้าถึงข้อมูล รวมถึงการประมวลผล การรักษาความปลอดภัยข้อมูล การรักษาความลับ และการยินยอมให้ผู้ควบคุมข้อมูลส่วนบุคคล ตรวจสอบการเผยแพร่ข้อมูล

๕.๒.๒.๓ (๓.๕) มอบหมายให้ทีมบริหารจัดการข้อมูล รับผิดชอบการดำเนินการและบันทึกประวัติการเผยแพร่ข้อมูล ตามอนุผนวก ๑๕ การบันทึกประวัติการเผยแพร่ข้อมูล (ISOC-DG-215) ประกอบผนวก ค สำหรับจัดทำเอกสารควบคุมหรือระบบบริหารจัดการทรัพย์สินข้อมูล เพื่อควบคุมการแก้ไข ปรับปรุง ตรวจสอบการส่งคืน หรือทำลายทรัพย์สินข้อมูลที่เผยแพร่ โดยเฉพาะข้อมูลที่มีความเสี่ยงสูง อย่างเป็นระบบ

๕.๒.๒.๓ (๔) ในกรณีเผยแพร่ข้อมูลในลักษณะเปิดเผยข้อมูลออกสู่สาธารณะ ให้ส่วนงานเจ้าของข้อมูล กำหนดมาตรการ อำนวยความสะดวกในการเผยแพร่ข้อมูล รวมทั้งควบคุมความปลอดภัยอย่างเหมาะสม ตามอนุผนวก ๖ มาตรการการเผยแพร่ข้อมูลออกสู่สาธารณะ (ISOC-DG-106) ประกอบผนวก ข ดังนี้

๕.๒.๒.๓ (๔.๑) รายละเอียดข้อมูลที่ทำการเผยแพร่ให้มีความชัดเจน รวมทั้งความปลอดภัยและระดับความเสี่ยง

๕.๒.๒.๓ (๔.๒) มาตรการและกำกับดูแลการรักษาความปลอดภัยและความเหมาะสมในการเผยแพร่ข้อมูล ซึ่งรวมถึงวิธีการ ช่องทางเผยแพร่ข้อมูลด้วย

๕.๒.๒.๓ (๔.๓) รักษาความปลอดภัยระหว่างการเผยแพร่ข้อมูลให้เหมาะสมเพียงพอต่อระดับความเสี่ยงของข้อมูล

๕.๒.๒.๓ (๔.๔) จัดทำเอกสารควบคุมการเผยแพร่ รวมทั้งกำกับให้เจ้าหน้าที่ควบคุมข้อมูล กำกับดูแลการเผยแพร่ข้อมูลด้วย

๕.๒.๒.๓ (๕) ให้ส่วนงานเจ้าของข้อมูล กำหนดมาตรการควบคุมและรักษาความปลอดภัยเพิ่มเติม กรณีข้อมูลที่มีความอ่อนไหว ข้อมูลที่ส่งผลกระทบต่อความมั่นคงของชาติ ข้อมูลที่อาจส่งผลกระทบต่อสิทธิและเสรีภาพของบุคคล หรือข้อมูลความลับทางราชการ ดังนี้

๕.๒.๒.๓ (๕.๑) ประสานศูนย์ดิจิทัลเพื่อความมั่นคง กอ.รมน. ร่วมตรวจสอบและประเมินสภาพแวดล้อมการรักษาความปลอดภัยของระบบเครือข่ายคอมพิวเตอร์ของผู้ใช้งานข้อมูล เพื่อนำผลไปใช้ประกอบในการพิจารณาการกำหนดสิทธิ

๕.๒.๒.๓ (๕.๒) ก่อนการอนุมัติสิทธิในการเข้าถึงข้อมูลให้กับผู้ใช้งานข้อมูล ต้องตรวจสอบรายละเอียดตามแนวทางหรือมาตรฐานที่คณะกรรมการธรรมาภิบาลข้อมูล กอ.รมน. กำหนด ทั้งนี้ต้องระงับสิทธิการเข้าถึงข้อมูลของผู้ใช้งาน เมื่อตรวจพบการไม่ปฏิบัติตามแนวทางหรือมาตรฐานที่กำหนด หรือมีเหตุอันควร ในทันที

๕.๒.๒.๓ (๕.๓) ให้เข้ารหัสข้อมูลตลอดระยะเวลาระหว่างการเผยแพร่ข้อมูล รวมทั้งตรวจสอบการดำเนินการตามมาตรการการเข้ารหัสข้อมูลที่กำหนด ตามแนวทางหรือมาตรฐานที่คณะกรรมธรรมาภิบาลข้อมูล กอ.รมน. เห็นชอบ ตามอนุผนวก ๗ การเข้ารหัสข้อมูล (ISOC-DG-107) ประกอบผนวก ข

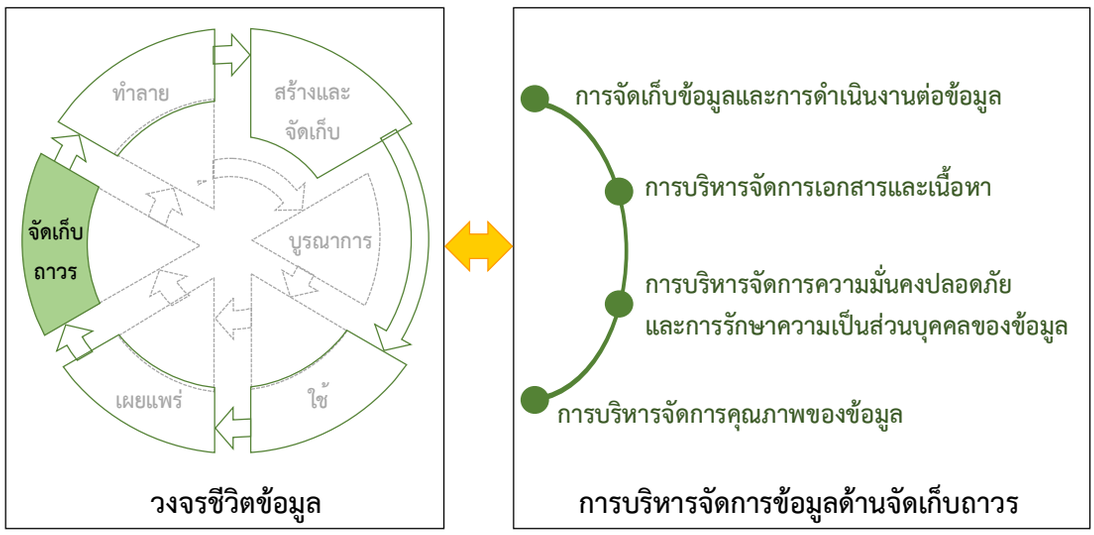
๕.๒.๒.๓ (๕.๔) ทั้งนี้ ส่วนงานเจ้าของข้อมูล ทีมบริหารจัดการข้อมูล และผู้ใช้งานข้อมูล ต้องพร้อมรับการตรวจสอบการเผยแพร่ข้อมูลดังกล่าวจากทีมบริกรข้อมูล กอ.รมน. หรือเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล เมื่อได้รับการประสาน

๕.๒.๒.๔ ขั้นตอนจัดเก็บถาวร

ในขั้นตอนจัดเก็บถาวร มีผู้ที่มีส่วนได้ส่วนเสีย และแนวปฏิบัติในแต่ละประเด็นขององค์ประกอบการบริหารจัดการข้อมูลด้านความมั่นคงที่เกี่ยวข้อง ได้แก่ การจัดเก็บและการดำเนินงานต่อข้อมูลที่มีโครงสร้าง และการบริหารจัดการเอกสารและเนื้อหาสำหรับข้อมูลแบบกึ่งโครงสร้างและไม่มีโครงสร้างที่ต้องกำหนดแนวทางการดำเนินการต่อข้อมูลที่ได้จัดเก็บไว้เกินระยะเวลาที่กำหนดตามขั้นตอนสร้างและจัดเก็บ รวมถึงข้อมูลที่ไม่มีการใช้งานแล้ว ด้วยวิธีการโอนย้ายข้อมูลเข้าไปจัดเก็บในพื้นที่จัดเก็บถาวร แต่ยังคงสามารถนำกลับมาใช้งานได้อีกเมื่อต้องการ ผ่านการบริหารจัดการความมั่นคงปลอดภัยและการรักษาความเป็นส่วนบุคคลของข้อมูล และการบริหารจัดการคุณภาพของข้อมูล อย่างเป็นระบบ ตามรูปที่ ๕.๖ ดังนี้

๕.๒.๒.๔ (๑) ผู้ที่มีส่วนได้ส่วนเสียในขั้นตอนจัดเก็บถาวร มีจำนวน ๖ กลุ่ม ประกอบด้วย : (๑) ส่วนงานเจ้าของข้อมูล (๒) ทีมบริหารจัดการข้อมูล (๓) ผู้ควบคุมข้อมูลส่วนบุคคล (๔) ทีมบริกรข้อมูล กอ.รมน. (๕) เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล และ (๖) ศูนย์ดิจิทัลเพื่อความมั่นคง กอ.รมน.

๕.๒.๒.๔ (๒) ให้ส่วนงานเจ้าของข้อมูล วางแผน กำหนดแนวทาง บริหารจัดการและดำเนินการเพื่อย้ายข้อมูลไปจัดเก็บถาวร ตามแนวทางหรือมาตรฐานที่คณะกรรมการธรรมาภิบาลข้อมูล กอ.รมน. กำหนด โดยมีการรักษาความมั่นคงปลอดภัย อย่างเป็นระบบ ดังนี้



รูปที่ ๕.๖ ความสัมพันธ์การบริหารจัดการข้อมูลด้านจัดเก็บถาวร

๕.๒.๒.๔ (๒.๑) กำหนดวิธีการ ระบบ ขั้นตอน ช่วงเวลาในการจัดเก็บข้อมูลถาวร ทั้งนี้ให้ทดสอบวิธีการ ระบบ ขั้นตอน ในการจัดเก็บข้อมูลถาวรอย่างน้อยปีละ ๑ ครั้ง รวมทั้งก่อนการนำข้อมูลที่ได้จัดเก็บถาวร ต้องตรวจสอบคุณภาพ ความถูกต้องครบถ้วนสมบูรณ์ของข้อมูลก่อนทุกครั้ง

๕.๒.๒.๔ (๒.๒) จัดทำเอกสารควบคุมประวัติการจัดเก็บข้อมูลถาวร หรือระบบบริหารจัดการทรัพย์สินข้อมูลถาวร เพื่อควบคุมการโอนย้าย ห้วงเวลา การแก้ไขปรับปรุง การเรียกใช้งาน การโอนข้อมูลกลับ และการทำลายทรัพย์สินข้อมูลถาวร โดยเฉพาะข้อมูลที่มีความเสี่ยงสูงอย่างเป็นระบบ โดยใช้แบบฟอร์ม ตามอนุผนวก ๑๖ บัญชีคุมข้อมูลถาวร (ISOC-DG-216) ประกอบผนวก ค

๕.๒.๒.๔ (๒.๓) กำหนดมาตรการในการรักษาความปลอดภัยข้อมูลที่ทำการย้าย การลบข้อมูลเดิม การจัดเก็บถาวร รวมทั้งการรักษาความมั่นคงปลอดภัยไซเบอร์

๕.๒.๒.๔ (๒.๔) กำหนดเครื่องมือและพื้นที่ที่ใช้ในการจัดเก็บข้อมูลถาวร

๕.๒.๒.๔ (๓) ให้ส่วนงานเจ้าของข้อมูล กำหนดมาตรการควบคุมและรักษาความปลอดภัยเพิ่มเติม กรณีข้อมูลที่มีความอ่อนไหว ข้อมูลที่ส่งผลกระทบต่อความมั่นคงของชาติ ข้อมูลที่อาจส่งผลกระทบต่อสิทธิและเสรีภาพของบุคคล หรือข้อมูลความลับทางราชการ ดังนี้

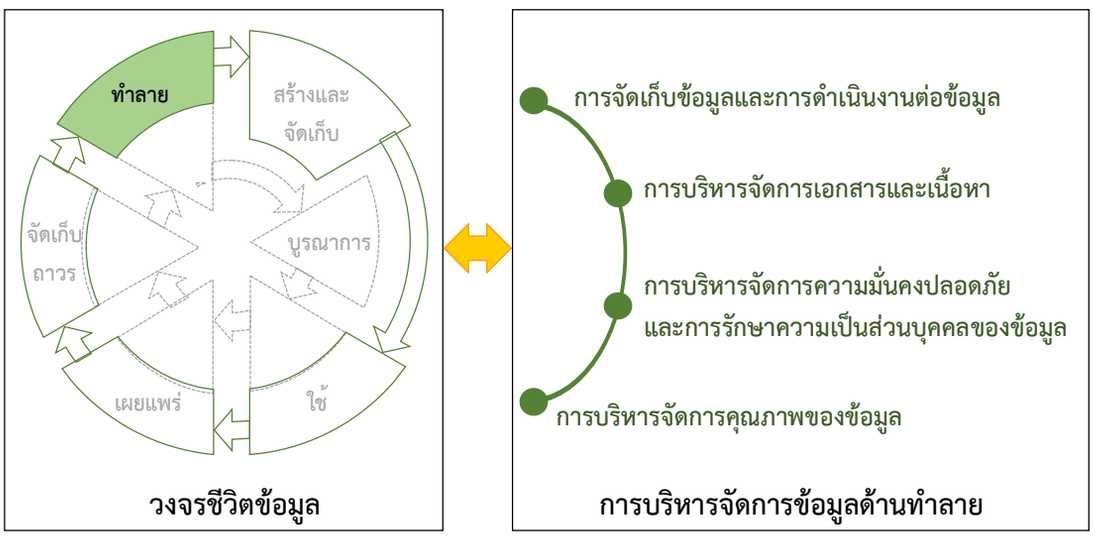
๕.๒.๒.๔ (๓.๑) ประสานศูนย์ดิจิทัลเพื่อความมั่นคง กอ.รมน. ร่วมตรวจสอบและประเมินสภาพแวดล้อมการรักษาความปลอดภัยของระบบเครือข่ายคอมพิวเตอร์สำหรับการจัดเก็บถาวร

๕.๒.๒.๔ (๓.๒) ให้เข้ารหัสข้อมูลตลอดระยะเวลาการจัดเก็บถาวร โดยตรวจสอบการดำเนินการตามมาตรการการเข้ารหัสข้อมูลที่กำหนด ตามแนวทางหรือมาตรฐานที่คณะกรรมการธรรมาภิบาลข้อมูล เห็นชอบ

๕.๒.๒.๔ (๔) ทั้งนี้ ส่วนงานเจ้าของข้อมูล และทีมบริหารจัดการข้อมูล ต้องพร้อมรับการตรวจสอบการจัดเก็บข้อมูลถาวรดังกล่าวจากทีมบริกรข้อมูล กอ.รมน. และเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล เมื่อได้รับการประสาน

๕.๒.๒.๕ ขั้นตอนทำลาย

ในขั้นตอนทำลาย มีผู้ที่มีส่วนได้ส่วนเสีย และแนวปฏิบัติในแต่ละประเด็นขององค์ประกอบการบริหารจัดการข้อมูลด้านความมั่นคงที่เกี่ยวข้อง ได้แก่ การจัดเก็บและการดำเนินงานต่อข้อมูล และการบริหารจัดการเอกสารและเนื้อหาข้อมูลของหน่วยงาน ซึ่งมีการจัดเก็บ การจัดเก็บถาวรเป็นระยะเวลานานหรือเกินกว่าระยะที่กำหนด หรือมีการร้องขอให้ทำลายข้อมูล ภายใต้การบริหารจัดการความมั่นคงปลอดภัยและการรักษาความเป็นส่วนบุคคลของข้อมูล ตามรูปที่ ๕.๗ ดังนี้



รูปที่ ๕.๗ ความสัมพันธ์การบริหารจัดการข้อมูลด้านทำลาย

๕.๒.๒.๕ (๑) ผู้ที่มีส่วนได้ส่วนเสียในขั้นตอนทำลาย มีจำนวน ๗ กลุ่ม ประกอบด้วย : (๑) หัวหน้าส่วนงานเจ้าของข้อมูล (๒) ส่วนงานเจ้าของข้อมูล (๓) เจ้าของข้อมูลส่วนบุคคล (๔) ทีมบริหารจัดการข้อมูล (๕) ทีมบริกรข้อมูล กอ.รมน. (๖) เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล และ (๗) คณะกรรมการทำลายข้อมูลประจำปี

๕.๒.๒.๕ (๒) ให้ส่วนงานเจ้าของข้อมูล ปฏิบัติให้เป็นไปตามกรอบระเบียบ กฎหมายที่เกี่ยวข้อง ได้แก่ ระเบียบสำนักนายกรัฐมนตรี ว่าด้วยงานสารบรรณ พ.ศ. ๒๕๒๖ และที่แก้ไขเพิ่มเติม โดยมีรายละเอียดการดำเนินการเกี่ยวกับข้อมูล (เพิ่มเติม) ในข้อ ๕.๒.๒.๕ (๓) - ๕.๒.๒.๕ (๖)

๕.๒.๒.๕ (๓) ให้ส่วนงานเจ้าของข้อมูล ตรวจสอบและจัดทำบัญชีขอทำลายข้อมูลที่ครบอายุการจัดเก็บตามที่ระบุในข้อ ๕.๒.๒.๑ (๕) และข้อ ๕.๒.๒.๔ (๒.๑) หรือข้อมูลที่เก็บไว้ไม่เกิดประโยชน์หรือข้อมูลไม่มีการใช้งานใด ๆ ภายใน ๖๐ วัน หลังจากวันสิ้นปีปฏิทิน ทั้งนี้ให้ตรวจสอบผลกระทบจากการทำลายข้อมูลใด ๆ ต้องไม่ส่งผลกระทบต่อคุณภาพของชุดข้อมูลที่ยังจัดเก็บและใช้งานอยู่ โดยใช้แบบฟอร์ม ตามอนุผนวก ๑๗ บัญชีขอทำลายข้อมูล (ISOC-DG-217) ประกอบผนวก ค

๕.๒.๒.๕ (๔) ให้ส่วนงานเจ้าของข้อมูล แต่งตั้งคณะกรรมการทำลายข้อมูลประจำปี โดยมี นายทหารสัญญาบัตร หรือข้าราชการพลเรือนระดับ ๓ หรือเทียบเท่าขึ้นไป จำนวน ๓ คนขึ้นไป เป็นองค์ประกอบคณะกรรมการฯ ดำเนินการดังนี้

๕.๒.๒.๕ (๔.๑) ทวนสอบบัญชีขอทำลายข้อมูล และให้ข้อเสนอแนะกรณีเห็นสมควรทำลาย หรือขยายระยะเวลาการจัดเก็บข้อมูล ให้หัวหน้าส่วนงานเจ้าของข้อมูล พิจารณาอนุมัติ ทั้งนี้ ในกรณีเสนอให้ขยายระยะเวลาการจัดเก็บ ให้ระบุห้วงระยะเวลาที่ขยายออกไปให้ชัดเจนด้วย โดยใช้แบบฟอร์ม ตามอนุผนวก ๑๘ บัญชีการทวนสอบขอทำลายข้อมูล (ISOC-DG-218) ประกอบผนวก ค

๕.๒.๒.๕ (๔.๒) ควบคุมกำกับดูแลการทำลายข้อมูลที่ได้รับอนุมัติให้ทำลาย จากระบบจัดเก็บข้อมูลทั้งหมด และเมื่อทำลายแล้วให้บันทึกรายงานให้หัวหน้าส่วนงานเจ้าของข้อมูลทราบ รวมทั้งแจ้งให้เจ้าของข้อมูลทราบ

๕.๒.๒.๕ (๕) ให้บันทึกสถานการณ์ทำลายข้อมูล ในเอกสารควบคุมประวัติการจัดเก็บข้อมูล/ข้อมูลถาวร หรือจากระบบบริหารจัดการ ทรัพย์สินข้อมูล/ข้อมูลถาวร ของส่วนงาน เพื่อให้สามารถตรวจสอบประวัติได้ในภายหลัง โดยใช้แบบฟอร์ม ตามอนุผนวก ๑๙ บัญชีคุมข้อมูลทำลาย (ISOC-DG-219) ประกอบผนวก ค

๕.๒.๒.๕ (๖) ทั้งนี้ ในกรณีที่การเก็บข้อมูลที่มีระดับชั้นความลับที่สุด และอาจเสี่ยงต่อการรั่วไหลอันจะเกิดอันตรายแก่ประโยชน์แห่งรัฐ หรือข้อมูลที่ส่งผลกระทบต่อความมั่นคงของชาติ ข้อมูลที่อาจส่งผลกระทบต่อสิทธิและเสรีภาพของบุคคล ให้ส่วนงานเจ้าของข้อมูล พิจารณาสั่งทำลายได้ หากเห็นว่ามีความจำเป็นอย่างยิ่ง โดยดำเนินการตามขั้นตอนในข้อ ๕.๒.๒.๕ (๔) และข้อ ๕.๒.๒.๕ (๕)

๕.๒.๒.๕ (๗) ทั้งนี้ ส่วนงานเจ้าของข้อมูล ทีมบริหารจัดการข้อมูล ต้องพร้อมรับการตรวจสอบการทำลายข้อมูลจากทีมบริกรข้อมูล กอ.รมน. และเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล เมื่อได้รับการประสาน

๕.๓ แนวปฏิบัติในการขับเคลื่อนการบริหารจัดการความเสี่ยง

แนวปฏิบัติในการขับเคลื่อนการบริหารจัดการความเสี่ยง จะต้องดำเนินการให้สอดคล้องกับระดับความเสี่ยงของข้อมูล โดยกำหนดระดับความเสี่ยงและความร้ายแรงของผลกระทบ (Impact Levels) แบ่งเป็นระดับต่ำ ระดับกลาง และระดับสูง ซึ่งมีความเกี่ยวข้องกับคุณภาพข้อมูลในทุกขั้นตอนของวงจรชีวิตข้อมูล โดยผู้ที่มีส่วนได้ส่วนเสีย พึงตระหนักและเตรียมการล่วงหน้า ให้สามารถปฏิบัติได้ในทันทีที่เกิดเหตุการณ์ ทั้งนี้ ได้กำหนดปัจจัยที่มีอิทธิพลต่อความเสี่ยง ได้แก่ ความสำคัญของข้อมูล ระดับชั้นความลับ ความเป็นส่วนบุคคล ปริมาณหรือขนาดของข้อมูล จำนวนผู้ใช้งานและจำนวนกิจกรรมที่ใช้ข้อมูล ความอ่อนไหวของข้อมูล และผลกระทบต่อ ความมั่นคง เจ้าของข้อมูล หน่วยงานของรัฐหรือภาคเอกชนที่เกี่ยวข้อง รัฐบาล และประเทศ เป็นต้น

๕.๓.๑ ให้ส่วนงานเจ้าของข้อมูล ประเมินความเสี่ยงของข้อมูล เพื่อรวบรวมปัญหา ข้อบกพร่อง ช่องโหว่ ฯลฯ ที่อาจเกิดขึ้นกับข้อมูลในแต่ละขั้นตอนบนวงจรชีวิตข้อมูล ทั้งที่เป็นแบบมีเจตนาและไม่มีเจตนา เพื่อนำไปใช้ประกอบการกำหนดมาตรการควบคุมความเสี่ยงและป้องกันเหตุการณ์ที่อาจมีผลกระทบต่อข้อมูล โดยใช้แบบฟอร์ม ตามอนุผนวก ๒๐ การประเมินความเสี่ยง (ISOC-DG-220) ประกอบผนวก ค ทั้งนี้ให้ทบทวนกระบวนการประเมินความเสี่ยง อย่างน้อยปีละ ๑ ครั้ง ในประเด็นดังต่อไปนี้

๕.๓.๑.๑ ระบุปัจจัยที่มีอิทธิพลต่อความเสี่ยง ต้นเหตุ หรือบ่อเกิดแห่งเหตุการณ์ของความเสี่ยง เช่น การเข้าถึงระบบโดยมิชอบ หรือการดัดแปลงข้อมูล เป็นต้น

๕.๓.๑.๒ ระบุระดับความน่าจะเป็นของเหตุการณ์ที่ทำให้เกิดความเสี่ยง เช่น โอกาสเกิดเหตุการณ์สูง กลาง หรือต่ำ

๕.๓.๑.๓ กำหนดระดับความเสี่ยงและความร้ายแรงของผลกระทบ

๕.๓.๑.๔ ระบุผลกระทบที่เกิดจากความเสี่ยง เช่น ทำให้เกิดความเสียหายแก่ชื่อเสียง ทำให้สูญเสียความลับ หรือทำให้ข้อมูลสามารถระบุความเป็นส่วนบุคคล เป็นต้น

๕.๓.๑.๕ กำหนดมาตรการเพื่อลดความเสี่ยง เช่น การเพิ่มมาตรการทางเทคโนโลยีเพื่อความปลอดภัย การฝึกอบรมบุคลากรให้สามารถประเมินความเสี่ยงและจัดการความเสี่ยงได้ และการแฝงข้อมูลหรือทำให้ข้อมูลไม่สามารถระบุตัวตนได้

๕.๓.๒ ให้ส่วนงานเจ้าของข้อมูล กำหนดขั้นตอนและแนวปฏิบัติเพื่อประเมินความพร้อมของการธรรมาภิบาลข้อมูลในแต่ละปัจจัยที่มีอิทธิพลต่อความเสี่ยง อย่างเป็นวงรอบ ตามอนุผนวก ๘ การประเมินความพร้อมการธรรมาภิบาลข้อมูล (ISOC-DG-108) ประกอบผนวก ข

๕.๓.๓ ให้ส่วนงานเจ้าของข้อมูล จัดทำแผนเตรียมความพร้อมกรณีเกิดเหตุฉุกเฉิน หรือแผนเผชิญเหตุเป็นรายกรณี (เช่นแผนเผชิญเหตุกรณีเกิดเหตุการณ์ข้อมูลรั่วไหล) เพื่อให้สามารถสกัดยับยั้ง กู้คืนข้อมูล หรือปรับแก้ไขปัญหา ฟื้นฟูสภาพแวดล้อมที่เกี่ยวข้องกับข้อมูล เพื่อให้สามารถนำข้อมูลกลับมาใช้งานได้ตามปกติโดยเร็ว อย่างมีคุณภาพ และไม่ส่งผลกระทบต่อภารกิจ ภาพลักษณ์ และความเชื่อมั่นของหน่วยงานของรัฐ ภาคเอกชน และสังคมทั่วไป ทั้งนี้แผนเตรียมความพร้อมกรณีเกิดเหตุฉุกเฉิน หรือแผนเผชิญเหตุต้องกำหนดรายละเอียด ตามอนุผนวก ๙ แผนเผชิญเหตุกรณีเกิดเหตุฉุกเฉิน (ISOC-DG-109) ประกอบผนวก ข อย่างน้อยดังนี้

๕.๓.๓.๑ กระบวนการปฏิบัติในการเผชิญเหตุการณ์

๕.๓.๓.๒ ผู้รับผิดชอบตามกระบวนการปฏิบัติในการเผชิญเหตุ

๕.๓.๓.๓ การรายงานเหตุและกรอบระยะเวลาในการรายงานให้หัวหน้าส่วนงานเจ้าของข้อมูลทราบ โดยมีรายละเอียดการรายงาน ดังนี้

๕.๓.๓.๓ (๑) คำอธิบายลักษณะเหตุการณ์

๕.๓.๓.๓ (๒) ผลที่อาจเกิดขึ้นจากเหตุการณ์ ความเสี่ยงต่อเจ้าของข้อมูล

๕.๓.๓.๓ (๓) มาตรการที่เสนอแนะหรือแนวทางบรรเทาเหตุ หรือผลกระทบที่อาจเกิดขึ้น

๕.๓.๓.๓ (๔) ผู้ประสานหรือเจ้าหน้าที่ติดต่อเพื่อสอบถามข้อมูลเหตุการณ์

๕.๓.๓.๔ กำหนดแนวทางการเปลี่ยนแปลงการปฏิบัติด้านข้อมูลที่เกี่ยวข้องในระหว่างการดำเนินการเผชิญเหตุ

๕.๓.๓.๕ สรุปรายงานเหตุการณ์ และนำสาเหตุการเกิดเหตุการณ์มาวิเคราะห์เพื่อหาแนวทางในการป้องกันการเกิดเหตุ

๕.๓.๔ เมื่อเกิดเหตุฉุกเฉินที่มีความเสี่ยงต่อข้อมูล ให้ดำเนินการดังนี้

๕.๓.๔.๑ ให้ผู้ตรวจพบแจ้งให้ผู้รับผิดชอบตามกระบวนการปฏิบัติในการเผชิญเหตุ หรือผู้ประสานหรือเจ้าหน้าที่ติดต่อเพื่อสอบถามข้อมูลเหตุการณ์ ทราบ เพื่อดำเนินการตามกระบวนการปฏิบัติในการเผชิญเหตุการณ์นั้น ๆ ตามข้อ ๕.๓.๓.๑

๕.๓.๔.๒ ให้ผู้รับผิดชอบตามกระบวนการปฏิบัติในการเผชิญเหตุ ประเมินความเสี่ยงและผลกระทบในทันที โดยใช้แบบฟอร์ม ตามอนุผนวก ๒๑ การประเมินความเสี่ยงภัยและผลกระทบ (ISOC-DG-221) ประกอบผนวก ค

๕.๓.๔.๓ ให้ผู้ประสานหรือเจ้าหน้าที่ติดต่อเพื่อสอบถามข้อมูลเหตุการณ์ แจ้งรายละเอียดและผลกระทบแก่ผู้ใช้งานข้อมูล และผู้มีส่วนได้ส่วนเสีย จนกว่าสถานการณ์จะคลี่คลายหรือกลับมาเป็นปกติ ทั้งนี้ ให้รวบรวมรายละเอียดเกี่ยวกับเหตุการณ์ หรือหลักฐานทางดิจิทัลต่าง ๆ เพื่อใช้ประกอบการกำหนดมาตรการป้องกันการเกิดเหตุการณ์ซ้ำ

๕.๔ แนวปฏิบัติด้านการวัดและประเมินผลการขับเคลื่อนการดำเนินการ

วัตถุประสงค์หลักของวัดและประเมินผลการขับเคลื่อนการดำเนินการ เพื่อให้มีระบบประเมินความพร้อมในการธรรมาภิบาลข้อมูล รวมทั้งมีการตรวจสอบรายละเอียด ทิศทางการปฏิบัติให้เป็นไปตามเป้าหมาย และตัวชี้วัดที่ส่วนงานเจ้าของข้อมูลได้กำหนดไว้ ทั้งในมิติด้านนโยบาย มาตรฐาน การดำเนินการ ผลสัมฤทธิ์ และผลกระทบจากการดำเนินการธรรมาภิบาลข้อมูลที่อยู่ในกรอบความรับผิดชอบ เพื่อให้มีหลักฐานเชิงประจักษ์อันนำไปสู่การปรับปรุงแก้ไข ยกระดับธรรมาภิบาลข้อมูล ให้มีมาตรฐาน เป็นสากล เชื่อถือได้ อย่างเป็นรูปธรรม ดังนั้นจึงกำหนดขอบเขตงานดังต่อไปนี้

๕.๔.๑ ผู้ที่มีส่วนได้ส่วนเสียในกระบวนการ มีจำนวน ๑๐ กลุ่ม ประกอบด้วย : (๑) ส่วนงานเจ้าของข้อมูล (๒) คณะกรรมการประเมินความพร้อมและการดำเนินการธรรมาภิบาลข้อมูล (๓) ทีมบริหารจัดการข้อมูล (๔) ทีมบริกรข้อมูล กอ.รมน. (๕) เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (๖) ผู้สร้างข้อมูล (๗) ผู้ใช้งานข้อมูล (๘) เจ้าของข้อมูลส่วนบุคคล (๙) ผู้ประสานหรือเจ้าหน้าที่ติดต่อเพื่อสอบถามข้อมูลเหตุการณ์ และ (๑๐) ผู้มีส่วนได้ส่วนเสียอื่นๆ

๕.๔.๒ ให้ส่วนงานเจ้าของข้อมูล แต่งตั้งคณะกรรมการประเมินความพร้อมและการดำเนินการธรรมาภิบาลข้อมูล มีหน้าที่ตรวจสอบ วัดผล และประเมินความพร้อมและการดำเนินการเกี่ยวกับการธรรมาภิบาลข้อมูล ภายใต้กรอบเป้าหมาย และตัวชี้วัดด้านนโยบาย มาตรฐาน และแนวปฏิบัติที่อยู่ในกรอบความรับผิดชอบของส่วนงาน โดยมีองค์ประกอบ ดังนี้

๕.๔.๒.๑ ประธานกรรมการ เป็นนายทหารสัญญาบัตรระดับชั้นยศ พันเอก หรือข้าราชการพลเรือนระดับ ๘ หรือเทียบเท่าขึ้นไป

๕.๔.๒.๒ กรรมการ และเลขานุการ เป็นนายทหารระดับสัญญาบัตร หรือข้าราชการพลเรือนระดับ ๘ หรือเทียบเท่าขึ้นไป จำนวนไม่น้อยกว่า ๔ คน

๕.๔.๓ ให้คณะกรรมการประเมินความพร้อมและการดำเนินการธรรมาภิบาลข้อมูล จัดทำแผนและดำเนินการ เพื่อตรวจสอบ วัดผล และประเมินความพร้อม รวมถึงผลการปฏิบัติในทุกขั้นตอนการธรรมาภิบาลของวงจรชีวิตข้อมูล ในข้อ ๕.๒ - ๕.๓ ทั้งนี้ให้ความสำคัญในเรื่อง การรักษาความมั่นคงปลอดภัย การคุ้มครองข้อมูลส่วนบุคคล การป้องกันการรั่วไหล คุณภาพข้อมูล และการเก็บประวัติหลักฐาน เป็นสำคัญ โดยสรุปรายงานผลการปฏิบัติประจำปีงบประมาณ ให้หัวหน้าส่วนงานเจ้าของข้อมูลทราบ ตามอนุผนวก ๑๐ รายงานการปฏิบัติด้านการธรรมาภิบาลข้อมูล (ISOC-DG-110) ประกอบผนวก ข

๕.๔.๔ ให้ผู้ที่มีความเกี่ยวข้องในส่วนงาน รับทราบผลการตรวจสอบ วัดผล และประเมินความพร้อม หรือผลการปฏิบัติ และร่วมมือกับคณะกรรมการประเมินความพร้อมและการดำเนินการธรรมาภิบาลข้อมูล เพื่อจัดทำแผนดำเนินการเพื่อแก้ไขและป้องกัน (Corrective and Preventive Action Plan : CPAP) รวมทั้ง ปรับเป้าหมายและตัวชี้วัดการธรรมาภิบาลข้อมูลของส่วนงาน ที่สะท้อนข้อเท็จจริงจากผลการตรวจสอบ วัดผล และประเมิน และสอดคล้องกับแนวทางนโยบายที่คณะกรรมการธรรมาภิบาลข้อมูลได้ให้ความเห็นชอบ เพื่อยกระดับการธรรมาภิบาลข้อมูลของส่วนงาน ในห้วงระยะต่อไป ก่อนเสนอให้หัวหน้าส่วนงานเจ้าของข้อมูล พิจารณาอนุมัติ ตามอนุผนวก ๒๒ แบบฟอร์มการแก้ไขและป้องกัน (ISOC-DG-222) ประกอบผนวก ค

บทที่ ๕ เป็นการชี้แจงรายละเอียดเกี่ยวกับการกำหนดขอบเขตงาน ขั้นตอนการปฏิบัติของผู้ที่มีส่วนได้ส่วนเสีย กับการธรรมาภิบาลข้อมูล ในระดับส่วนงานของ กอ.รมน. ซึ่งครอบคลุมการกำหนดทิศทาง เป้าหมาย และการปฏิบัติ ทั้งในด้านการขับเคลื่อนงานยามปกติ การบริหารจัดการความเสี่ยงในสถานการณ์ฉุกเฉิน และการวัดและประเมินผล ที่นำไปสู่การปรับปรุงพัฒนาอย่างเป็นวงรอบต่อเนื่อง อย่างไรก็ตาม การที่จะขับเคลื่อนการดำเนินการให้สามารถ บรรลุเป้าหมายที่กำหนดไว้ หน่วยงานเจ้าของข้อมูลซึ่งเป็นหน่วยรับผิดชอบหลัก จำเป็นต้องประชาสัมพันธ์ อบรม หรือมีกิจกรรมเพื่อเสริมสร้างความตระหนักรู้ ความเข้าใจ และพัฒนาทักษะประสบการณ์ ให้กับผู้ที่มีส่วนได้ ส่วนเสีย ในทุกขั้นตอนการปฏิบัติของวงจรชีวิตข้อมูล เพื่อให้เกิดความเชื่อมั่น ได้รับความเชื่อถือ และเป็นที่ยอมรับ จากทุกหน่วยงานและบุคลากรที่เกี่ยวข้อง ทั้งในด้านความชัดเจนในขั้นตอนปฏิบัติ การรักษาความปลอดภัย การรักษาชั้นความลับ การคุ้มครองข้อมูลส่วนบุคคล และความน่าเชื่อถือในคุณภาพข้อมูลที่ต้องมีความถูกต้อง ครบถ้วน สอดคล้องต้องกัน เป็นปัจจุบัน ตรงตามความต้องการ และพร้อมใช้งาน

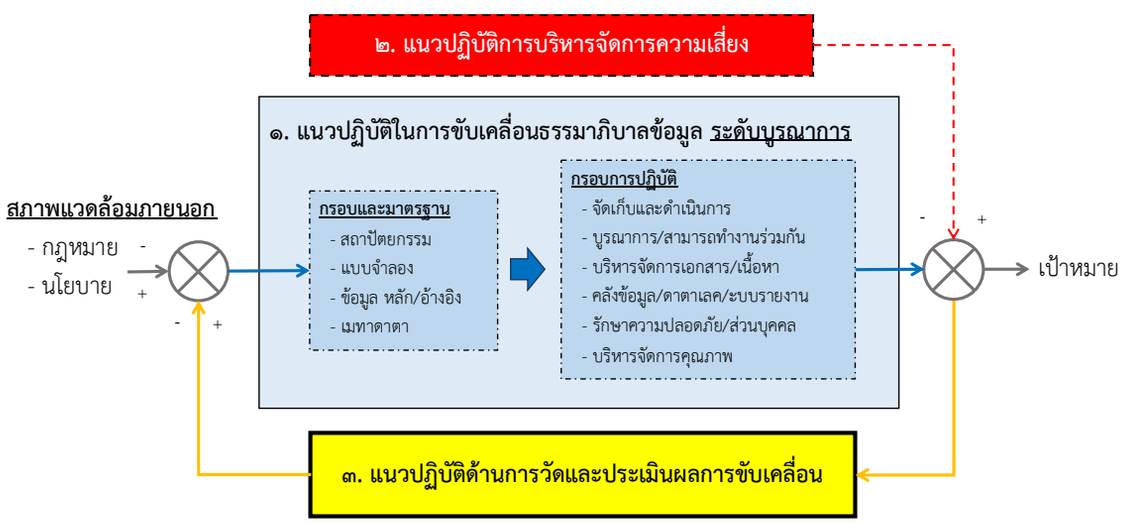
อย่างไรก็ตาม แม้ว่าส่วนงานของ กอ.รมน. ซึ่งมีฐานะเป็นส่วนงานเจ้าของข้อมูล จะเป็นหน่วยรับผิดชอบหลัก ในการธรรมาภิบาลข้อมูลภายในส่วนงานตนเอง แต่ก็จำเป็นต้องดำเนินการให้มีความประสานสอดคล้องกับนโยบาย แนวปฏิบัติ การบูรณาการและใช้งานข้อมูลของ กอ.รมน. ซึ่งได้มอบหมายให้ผู้บริหารระดับสูง กอ.รมน. และผู้บริหารข้อมูลระดับสูง เป็นผู้รับผิดชอบตามลำดับ โดยมีคณะกรรมการธรรมาภิบาลข้อมูล กอ.รมน. และมีทีมบริกรข้อมูล กอ.รมน. เป็นกลไกในการขับเคลื่อน ติดตาม และตรวจสอบการดำเนินการของแต่ละส่วนงาน เจ้าของข้อมูล ในภาพรวม อย่างเป็นระบบ ซึ่งจะได้กล่าวในบทที่ ๖ ต่อไป

บทที่ ๖
การธรรมาภิบาลข้อมูลระดับบูรณาการ

๖.๑ กล่าวนำ

การธรรมาภิบาลข้อมูลระดับบูรณาการ มีวัตถุประสงค์เพื่อขับเคลื่อนการบริหารจัดการข้อมูลที่ กอ.รมน. ในฐานะศูนย์กลางข้อมูลด้านความมั่นคงและผู้ประมวลผลข้อมูลส่วนบุคคล ได้เชื่อมโยงแลกเปลี่ยนมาจากหน่วยงานของรัฐและภาคเอกชน ให้ดี มีคุณภาพ และปลอดภัย ภายใต้บทบาทและความรับผิดชอบตามที่แผนปฏิบัติการด้านการบูรณาการข้อมูลด้านความมั่นคงฯ ได้กำหนด โดยจัดทำให้อยู่ในรูปแบบแนวปฏิบัติ พร้อมรายละเอียดการดำเนินการในแต่ละองค์ประกอบการบริหารจัดการข้อมูลในแต่ละขั้นตอนบนวงจรชีวิตข้อมูลระดับบูรณาการ ได้แก่ ขั้นตอนบูรณาการ จัดเก็บ ใช้ เผยแพร่ จัดเก็บถาวร และทำลาย เพื่อให้ผู้ที่มีส่วนได้ส่วนเสีย มีความตระหนักรู้เข้าใจ และสามารถนำไปใช้ยึดถือและขยายผลการปฏิบัติได้อย่างมั่นใจ เชื่อมั่น อย่างต่อเนื่อง

ทั้งนี้ เพื่อให้เกิดความชัดเจน ได้จัดกลุ่มแนวปฏิบัติ แบ่งออกเป็น ๓ ด้าน ตามรูปที่ ๖.๑ ประกอบด้วย



รูปที่ ๖.๑ กรอบงานธรรมาภิบาลข้อมูลระดับบูรณาการ

๖.๑.๑ แนวปฏิบัติในการขับเคลื่อนธรรมาภิบาลข้อมูลระดับบูรณาการ : เป็นแนวปฏิบัติในยามปกติ เพื่อให้เกิดธรรมาภิบาลข้อมูล ผ่านกระบวนการเตรียมการ การบริหารจัดการ และการนำไปสู่การปฏิบัติ ที่เป็นรูปธรรม

๖.๑.๒ แนวปฏิบัติการบริหารจัดการความเสี่ยง : เป็นแนวปฏิบัติเพื่อให้เกิดธรรมาภิบาลข้อมูลในยามที่เกิดเหตุผิดปกติ ฉุกเฉิน โดยให้ความสำคัญกับเหตุการณ์กรณีเกิดการรั่วไหลของข้อมูล และส่งผลกระทบร้ายแรงต่อความมั่นคงของประเทศ ความรับผิดชอบทางด้านกฎหมาย รวมถึงความเชื่อมั่นต่อ กอ.รมน. และระบบธรรมาภิบาลข้อมูลระดับบูรณาการของ กอ.รมน.

๖.๑.๓ แนวปฏิบัติด้านการวัดและประเมินผลการขับเคลื่อนการดำเนินการ : เป็นแนวปฏิบัติเพื่อให้เกิดการตรวจสอบวัดผล ทั้งในด้านคุณภาพและประสิทธิภาพของการธรรมาภิบาลข้อมูลระดับบูรณาการของ กอ.รมน. อย่างเป็นภาพรวม อันเป็นหนึ่งในกระบวนการของวงจรเดมมิ่ง (Deming Cycle) ที่กล่าวในบทที่ ๓ เพื่อประเมินเปรียบเทียบกับวัตถุประสงค์เป้าหมาย มาตรฐาน และแนวปฏิบัติ ที่ได้กำหนดขึ้นในห้วงต้นของการดำเนินการ เพื่อนำไปสู่การปรับปรุงแก้ไขอย่างเป็นระบบต่อเนื่องต่อไป

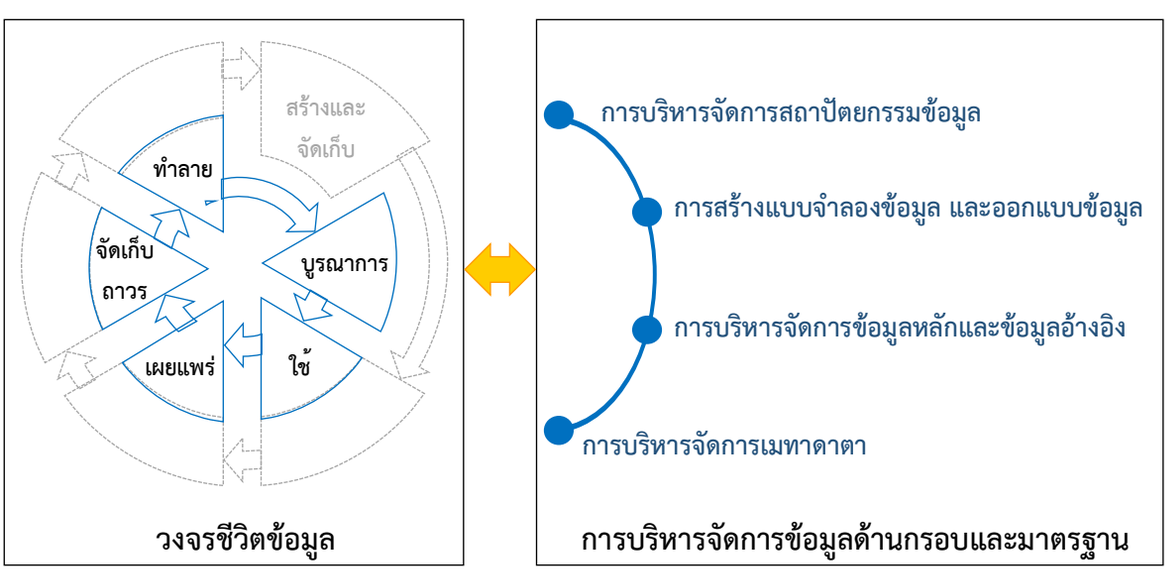
๖.๒ แนวปฏิบัติในการขับเคลื่อนธรรมาภิบาลข้อมูลระดับบูรณาการ

๖.๒.๑ การกำหนดกรอบและมาตรฐาน

การกำหนดกรอบและมาตรฐาน เป็นการดำเนินการภายใต้องค์ประกอบการบริหารจัดการข้อมูลด้านการบริหารจัดการสถาปัตยกรรมข้อมูล การสร้างแบบจำลองและออกแบบข้อมูล การบริหารจัดการข้อมูลหลักและข้อมูลอ้างอิง การบริหารจัดการความมั่นคงปลอดภัยและการรักษาความเป็นส่วนบุคคลของข้อมูล และการบริหารจัดการเมทาดาตา ตามรูปที่ ๖.๒ โดยให้ส่วนงานบริหารจัดการข้อมูล ตรวจสอบแนวทางเกี่ยวข้องที่ได้รับอนุมัติ หรือคณะกรรมการธรรมาภิบาลข้อมูล กอ.รมน. ได้ให้ความเห็นชอบ ความต้องการใช้งานข้อมูล และสภาพแวดล้อมที่เกี่ยวข้องกับข้อมูลทั้งหมด (ทั้งที่เป็นข้อมูลแบบมีโครงสร้าง แบบกึ่งโครงสร้าง และแบบไม่มีโครงสร้าง) และสรุปจัดทำเป็นแผนผัง แบบจำลองชุดข้อมูล พร้อมคำอธิบาย เพื่อให้ผู้ที่มีส่วนได้ส่วนเสีย เข้าใจและสามารถนำไปใช้ขยายผลในการดำเนินการต่อข้อมูลต่อไป ทั้งนี้ มีประเด็นที่ส่วนงานบริหารจัดการข้อมูล ต้องดำเนินการ สรุปได้ดังนี้

๖.๒.๑.๑ ผู้ที่มีส่วนได้ส่วนเสียในกระบวนการ มีจำนวน ๗ กลุ่ม ประกอบด้วย : (๑) ส่วนงานบริหารจัดการข้อมูล (๒) ผู้ประมวลผลข้อมูลส่วนบุคคล (๓) ทีมบริหารจัดการข้อมูล (๔) ส่วนงานเจ้าของข้อมูล (๕) หน่วยงานเจ้าของข้อมูล (๖) ผู้ใช้งานข้อมูล และ (๗) เจ้าของข้อมูลส่วนบุคคล

๖.๒.๑.๒ จัดทำแบบจำลองสำหรับการออกแบบข้อมูล ในรูปไดอะแกรม (Diagram) หรือตารางข้อมูล ตามอนุผนวก ๑ การจัดทำแบบจำลองสำหรับการออกแบบข้อมูล (NSDC-DG-301) ประกอบผนวก ง



รูปที่ ๖.๒ การกำหนดกรอบและมาตรฐานธรรมาภิบาลบนวงจรชีวิตข้อมูล

๖.๒.๑.๓ จัดทำมาตรฐานข้อมูล โดยกำหนดข้อมูลหลักและข้อมูลอ้างอิงที่ใช้งานโดยส่วนงานบริหารจัดการข้อมูลทั้งหมด ตามอนุผนวก ๒ การจัดทำมาตรฐานข้อมูล (NSDC-DG-302) ประกอบผนวก ง

๖.๒.๑.๔ ประเมินความเสี่ยง และกำหนดระดับความเสี่ยงและระดับชั้นความลับของข้อมูลที่ใช้งานโดยส่วนงานบริหารจัดการข้อมูล ให้มีความชัดเจน โดยใช้แบบฟอร์ม ตามอนุผนวก ๑ การประเมินความเสี่ยงของข้อมูล (NSDC-DG-201) ประกอบผนวก ค

๖.๒.๑.๕ จัดทำเมทาดาตา หรือคำอธิบายข้อมูลหลักและกลุ่มข้อมูลอื่น ๆ (ถ้ามี) โดยใช้แบบฟอร์มตามอนุผนวก ๒ แบบฟอร์มเมทาดาตา (NSDC-DG-202) ประกอบผนวก ค

๖.๒.๑.๖ จัดทำสถาปัตยกรรมข้อมูล ที่ระบุวัตถุประสงค์ เป้าหมาย และตัวชี้วัดเกี่ยวกับข้อมูล โครงสร้างหมวดหมู่ ประเภท ระดับชั้นความลับ และการเชื่อมโยงแลกเปลี่ยนข้อมูล รวมทั้งแผนผังภาพรวมแสดงความสัมพันธ์ การเชื่อมโยงและการไหลของข้อมูล ที่ส่วนงานบริหารจัดการข้อมูลต้องมีหรือควรมีใช้สนับสนุนการปฏิบัติภารกิจ ที่เป็นปัจจุบัน และรวมถึงแผนความต้องการใช้งานข้อมูลในอนาคต ตามอนุผนวก ๓ การจัดทำสถาปัตยกรรมข้อมูล (NSDC-DG-303) ประกอบผนวก ง

๖.๒.๑.๗ จัดทำระเบียบ ข้อตกลง มาตรฐาน เป้าหมาย และตัวชี้วัดการสร้างข้อมูล รวมทั้งการเชื่อมโยงแลกเปลี่ยน จัดเก็บ จัดเก็บถาวร โอนย้าย เผยแพร่ ใช้ ประมวลผล หรือดำเนินการใด ๆ ต่อข้อมูลภายใน กอ.รมน. ระหว่าง กอ.รมน. กับหน่วยงานของรัฐต่าง ๆ หรือ ระหว่าง กอ.รมน. กับภาคเอกชน หรือบุคคลที่เกี่ยวข้อง ให้มีความชัดเจนและปลอดภัย ตามอนุผนวก ๒ การสร้าง จัดเก็บ และจัดเก็บถาวร (NSDC-DG-101) ประกอบผนวก ข

๖.๒.๑.๘ จัดทำระเบียบ ข้อปฏิบัติ มาตรฐาน เป้าหมาย และตัวชี้วัดด้านการรักษาความปลอดภัยเกี่ยวกับข้อมูลที่อยู่ในความครอบครองของส่วนงานบริหารจัดการข้อมูล ในทุกขั้นตอน ตามระดับความเสี่ยงและระดับชั้นความลับ อย่างเหมาะสม ตามอนุผนวก ๒ การรักษาความปลอดภัยเกี่ยวกับข้อมูล (NSDC-DG-102) ประกอบผนวก ข

๖.๒.๑.๙ จัดทำระเบียบ ข้อปฏิบัติ มาตรฐาน เป้าหมาย และตัวชี้วัดด้านการคุ้มครองข้อมูลส่วนบุคคล ในทุกขั้นตอนของวงจรชีวิตข้อมูล ได้แก่ การสร้างและจัดเก็บ ใช้ เผยแพร่ จัดเก็บถาวร และทำลาย หรือการดำเนินการใด ๆ ต่อข้อมูลส่วนบุคคล โดยต้องเป็นไปตามข้อตกลง หรือกระบวนการยินยอมของเจ้าของข้อมูลส่วนบุคคล และต้องไม่ฝ่าฝืนหรือขัดต่อระเบียบ กฎหมาย และแนวทางที่ผู้ควบคุมข้อมูลส่วนบุคคลกำหนด อีกทั้งต้องสามารถป้องกันการสูญหาย ถูกทำลาย ถูกปลอมแปลง ถูกเปิดเผยหรือถูกเข้าถึงจากผู้ไม่ได้รับอนุญาต หรือทำให้ข้อมูลสามารถระบุถึงตัวบุคคลได้ ตามอนุผนวก ๓ การคุ้มครองข้อมูลส่วนบุคคล (NSDC-DG-103) ประกอบผนวก ข

๖.๒.๑.๑๐ จัดทำระเบียบ ข้อปฏิบัติ มาตรฐาน เป้าหมาย และตัวชี้วัดด้านคุณภาพข้อมูลทั้งระบบ ตั้งแต่การกำหนดเป้าหมาย การประเมิน การวิเคราะห์ การวางแผน การปรับปรุง และการควบคุมคุณภาพข้อมูลอยู่ในความครอบครองของส่วนงานบริหารจัดการข้อมูล เพื่อให้มีความถูกต้อง ครบถ้วน สอดคล้องต้องกัน เป็นปัจจุบัน ตรงความต้องการใช้งาน และมีความพร้อมใช้งาน ตามอนุผนวก ๔ การควบคุมคุณภาพข้อมูล (NSDC-DG-104) ประกอบผนวก ข

๖.๒.๑.๑๑ แต่งตั้งทีมบริหารจัดการข้อมูล ให้มีหน้าที่และอำนาจ ดังต่อไปนี้

๖.๒.๑.๑๑ (๑) สร้าง จัดเก็บ เชื่อมโยงแลกเปลี่ยน ใช้ สำรองและกู้คืน จัดเก็บถาวร เผยแพร่ และทำลายข้อมูลที่อยู่ในความรับผิดชอบ

๖.๒.๑.๑๑ (๒) กำกับดูแลการรักษาความปลอดภัย การจัดเก็บ ป้องกันการสูญหาย เข้าถึง ใช้ เปลี่ยนแปลง แก้ไข แลกเปลี่ยน โอนย้าย เปิดเผย หรือทำลายข้อมูลส่วนบุคคล ให้เป็นไปตามระเบียบ กฎหมาย และแนวทางที่ผู้ควบคุมข้อมูลส่วนบุคคลกำหนด โดยบันทึกรายการเพื่อให้เจ้าของข้อมูลส่วนบุคคล และส่วนงานหรือหน่วยงานที่สนับสนุนข้อมูลส่วนบุคคล สามารถตรวจสอบได้

๖.๒.๑.๑๒ ติดตาม ตรวจสอบสภาพแวดล้อมการดำเนินการ รวมถึงความต้องการใช้งาน (เพิ่มเติม) รวมทั้งกำกับดูแลการใช้งานข้อมูล อย่างต่อเนื่อง อีกทั้งกำหนดให้ทบทวน ปรับปรุงความถูกต้องและความทันสมัยในข้อ ๖.๒.๑.๒ – ๖.๒.๑.๑๑ ให้มีความเหมาะสม ในทันที่ที่มีการเปลี่ยนแปลง หรืออย่างน้อย ปีละ ๑ ครั้ง ดังนี้

๖.๒.๑.๑๒ (๑) บันทึกผลการตรวจสอบการปฏิบัติด้านข้อมูล โดยใช้แบบฟอร์มตามอนุผนวก ๓ การตรวจสอบการปฏิบัติด้านข้อมูล (NSDC-DG-203) ประกอบผนวก ค

๖.๒.๑.๑๒ (๒) บันทึกผลการตรวจสอบการรักษาความมั่นคงปลอดภัย โดยใช้แบบฟอร์มตามอนุผนวก ๔ การตรวจสอบการรักษาความมั่นคงปลอดภัย (NSDC-DG-204) ประกอบผนวก ค

๖.๒.๑.๑๒ (๓) บันทึกผลการตรวจสอบการคุ้มครองข้อมูลส่วนบุคคล โดยใช้แบบฟอร์มตามอนุผนวก ๕ การตรวจสอบการคุ้มครองข้อมูลส่วนบุคคล (NSDC-DG-205) ประกอบผนวก ค

๖.๒.๑.๑๒ (๔) บันทึกผลการตรวจสอบการรักษาความปลอดภัยของระบบและเครือข่าย โดยใช้แบบฟอร์ม ตามอนุผนวก ๖ การตรวจสอบการรักษาความปลอดภัยของระบบและเครือข่าย (NSDC-DG-206) ประกอบผนวก ค

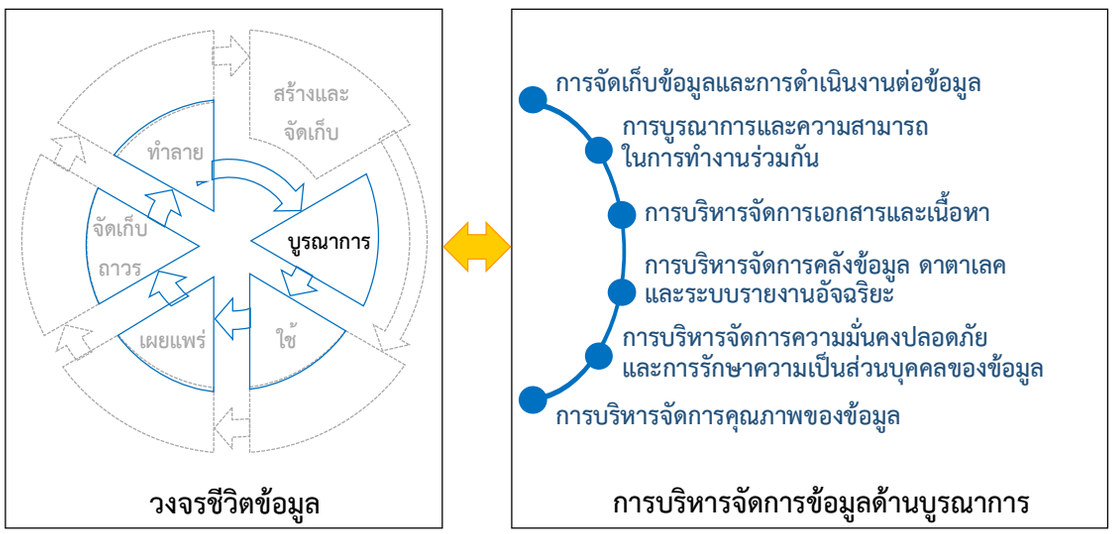
๖.๒.๒ การกำหนดกรอบการปฏิบัติ

ธรรมาภิบาลในวงจรชีวิตข้อมูลที่เกี่ยวข้องกับการนำไปสู่การปฏิบัติงานในกรอบหน้าที่และอำนาจของส่วนงานบริหารจัดการข้อมูล มีรวม ๕ ขั้นตอน ดังนี้

๖.๒.๒.๑ ขั้นตอนบูรณาการ

ในขั้นตอนบูรณาการ มีผู้ที่มีส่วนได้ส่วนเสีย และแนวปฏิบัติในแต่ละประเด็นขององค์ประกอบการบริหารจัดการข้อมูลด้านความมั่นคงที่เกี่ยวข้อง ได้แก่ การบูรณาการและความสามารถในการทำงานร่วมกัน การจัดเก็บและการดำเนินงานต่อข้อมูลที่มีโครงสร้าง การบริหารจัดการเอกสารและเนื้อหาข้อมูลแบบกึ่งโครงสร้างและแบบไม่มีโครงสร้าง การบริหารจัดการคลังข้อมูล ดาตาเลค และระบบรายงานอัจฉริยะ การบริหารจัดการความมั่นคงปลอดภัยและการรักษาความเป็นส่วนบุคคลของข้อมูล และการบริหารจัดการคุณภาพของข้อมูล ตามรูปที่ ๖.๓ ดังนี้

๖.๒.๒.๑ (๑) ผู้ที่มีส่วนได้ส่วนเสียในขั้นตอนบูรณาการ มีจำนวน ๗ กลุ่ม ประกอบด้วย : (๑) ส่วนงานบริหารจัดการข้อมูล (๒) ทีมบริหารจัดการข้อมูล (๓) ส่วนงานเจ้าของข้อมูล (๔) หน่วยงานเจ้าของข้อมูล (๕) เจ้าของข้อมูลส่วนบุคคล (๖) ทีมบริกรข้อมูล กอ.รมน. และ (๗) เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล



รูปที่ ๖.๓ ความสัมพันธ์การบริหารจัดการข้อมูลด้านบูรณาการ

๖.๒.๒.๑ (๒) ให้ส่วนงานบริหารจัดการข้อมูล กำหนดวิธีการดำเนินการ เครื่องมือและสภาพแวดล้อม สำหรับการบูรณาการข้อมูล ที่มีความเกี่ยวข้องกับความมั่นคง ร่วมกับส่วนงานหรือหน่วยงานเจ้าของข้อมูล รวมทั้งการบันทึกประวัติข้อมูล ให้มีความชัดเจน ปลอดภัย และเหมาะสมสอดคล้องกับผลประเมินระดับความเสี่ยงของข้อมูล รวมทั้งควบคุมคุณภาพของข้อมูล ให้เป็นไปตามเป้าหมาย แนวทาง ข้อปฏิบัติ ข้อกำหนด และมาตรฐานข้อมูลในข้อ ๖.๒.๑.๗ – ๖.๒.๑.๑๐ เช่น การจัดเก็บและรักษาข้อมูลที่มีความเสี่ยง ข้อมูลที่มีระดับชั้นความลับ และข้อมูลส่วนบุคคล ให้ทำการเข้ารหัสข้อมูลตามระดับความเสี่ยงของข้อมูลแต่ละประเภทด้วย เป็นต้น

๖.๒.๒.๑ (๓) ให้ส่วนงานบริหารจัดการข้อมูล กำหนดวิธีการดำเนินการ เครื่องมือและสภาพแวดล้อมกรณีมีหน่วยงานของรัฐอื่น ๆ ที่ไม่มีความเกี่ยวข้องกับความมั่นคง ร้องขอเชื่อมโยงแลกเปลี่ยน โอนย้ายข้อมูล โดยต้องขอนำเรียนอนุมัติผู้บริหารระดับสูง (CEO) และต้องจัดทำเป็นข้อตกลงการใช้งานข้อมูลระหว่างส่วนงานที่เกี่ยวข้อง โดยระบุวัตถุประสงค์ และรายละเอียดการขอใช้ข้อมูล ให้มีความชัดเจน ทั้งนี้ หากเป็นการแลกเปลี่ยนและเชื่อมโยงข้อมูลที่มีระดับชั้นความลับ หรือข้อมูลส่วนบุคคล จะต้องปฏิบัติตามมาตรการที่เกี่ยวข้อง อย่างเคร่งครัด

๖.๒.๒.๑ (๔) ให้ส่วนงานบริหารจัดการข้อมูล ประสานส่วนงานหรือหน่วยงานเจ้าของข้อมูล ปฏิบัติตามวิธีการ เครื่องมือ และสภาพแวดล้อมสำหรับการบูรณาการ เชื่อมโยงแลกเปลี่ยน และจัดเก็บข้อมูล ให้เป็นไปตามข้อตกลงร่วมระหว่าง กอ.รมน. กับส่วนงานหรือหน่วยงานเจ้าของข้อมูล ทั้งนี้ สำหรับกรณีการรวบรวมข้อมูลส่วนบุคคล ให้กำหนดวัตถุประสงค์ ระยะเวลาในการเก็บรวบรวม ประเภทของบุคคลหรือส่วนงาน หรือหน่วยงาน ที่อาจเข้าถึงหรือเปิดเผย สิทธิของเจ้าของข้อมูลส่วนบุคคลตามกฎหมายที่เกี่ยวข้องและรวมถึงข้อมูลเกี่ยวกับผู้ควบคุมข้อมูลส่วนบุคคล เพื่อให้เจ้าของข้อมูลส่วนบุคคลยินยอมก่อนหรือในขณะเก็บรวบรวมข้อมูลส่วนบุคคล

๖.๒.๒.๑ (๕) ให้ส่วนงานบริหารจัดการข้อมูล กำหนดห้วงระยะเวลาและดำเนินการจัดเก็บข้อมูล ตามแนวทางหรือมาตรฐานที่คณะกรรมธรรมาภิบาลข้อมูล กอ.รมน. เห็นชอบ (ภายใต้ข้อตกลงร่วมกับหน่วยงานเจ้าของข้อมูล) พร้อมทั้งบันทึกลงในบัญชีคุมข้อมูล ตามเงื่อนไข ดังนี้

๖.๒.๒.๑ (๕.๑) ระยะเวลาในการจัดเก็บจะต้องอยู่ภายใต้กรอบกฎหมาย ระเบียบข้อบังคับ หรือข้อตกลงระหว่างผู้ที่มีส่วนได้ส่วนเสียเกี่ยวกับการใช้ข้อมูล

๖.๒.๒.๑ (๕.๒) ระยะเวลาในการจัดเก็บจะต้องไม่นานเกินกว่าความจำเป็น

๖.๒.๒.๑ (๖) ให้ส่วนงานบริหารจัดการข้อมูล กำหนดวิธีการดำเนินการ เครื่องมือและสภาพแวดล้อม สำหรับการสำรองและกู้คืน ดังนี้

๖.๒.๒.๑ (๖.๑) กำหนดวิธีการหรือระบบ ขั้นตอน ช่วงเวลา สำหรับการสำรองและกู้คืนข้อมูล ทั้งนี้ให้ทดสอบวิธีการหรือระบบ ขั้นตอน สำหรับสำรองและกู้คืนข้อมูล อย่างน้อยปีละ ๑ ครั้ง รวมทั้งก่อนการนำข้อมูลที่ได้สำรองหรือกู้คืน ต้องตรวจสอบความถูกต้องครบถ้วนสมบูรณ์ของข้อมูลก่อนทุกครั้ง

๖.๒.๒.๑ (๖.๒) จัดทำบันทึกประวัติการสำรองหรือกู้คืนข้อมูล โดยระบุรายละเอียด ได้แก่ เวลาเริ่มต้นและสิ้นสุดในการดำเนินการ ชื่อเจ้าหน้าที่ผู้ดำเนินการ ประเภทและชั้นความลับของข้อมูล และรายละเอียดอื่น ๆ (เช่น ในกรณีที่เกิดข้อผิดพลาดในการสำรองหรือกู้คืนข้อมูล และวิธีดำเนินการแก้ไขข้อผิดพลาด เป็นต้น) ตามอนุผนวก ๗ การบันทึกประวัติการสำรองหรือกู้คืนข้อมูล (NSDC-DG-207) ประกอบผนวก ค

๖.๒.๒.๑ (๖.๓) หากมีความจำเป็นต้องทำการกู้คืนข้อมูล ให้ตรวจสอบคุณภาพข้อมูล และใช้ข้อมูลที่ทันสมัยที่สุด (Latest Update) ที่ได้สำรองไว้ หรือข้อมูลที่เหมาะสมที่สุด ทั้งนี้ต้องแจ้งความคืบหน้าการดำเนินการ ให้ส่วนงานหรือหน่วยงานเจ้าของข้อมูล ผู้ใช้งานข้อมูลและผู้ที่มีส่วนได้ส่วนเสีย ทราบอย่างต่อเนื่อง จนกว่าจะทำการกู้คืนข้อมูลเสร็จสิ้นอย่างสมบูรณ์

๖.๒.๒.๑ (๗) ให้ส่วนงานบริหารจัดการข้อมูล จัดทำบัญชีควบคุมข้อมูลที่บูรณาการเข้ามาจัดเก็บและเก็บรักษาพร้อมรับการตรวจจากทีมบริกรข้อมูล กอ.รมน. และเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลเมื่อได้รับการประสาน ดังนี้

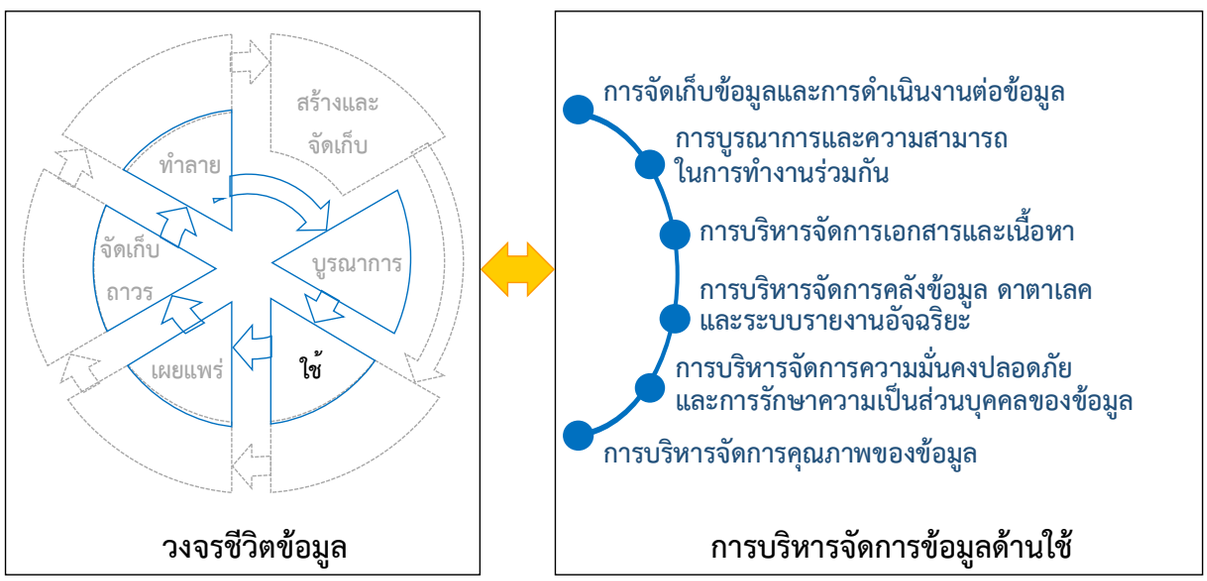
๖.๒.๒.๑ (๗.๑) บัญชีควบคุมการสร้างข้อมูล บันทึกและเก็บรักษารายการข้อมูลที่ไม่มีชั้นความลับ โดยใช้แบบฟอร์ม ตามอนุผนวก ๘ บัญชีคุมข้อมูลปกติ (NSDC-DG-208) ประกอบผนวก ค

๖.๒.๒.๑ (๗.๒) บัญชีควบคุมรายการชุดข้อมูลที่มีชั้นความลับและต้องการดูแลเป็นกรณีพิเศษ โดยใช้แบบฟอร์ม ตามอนุผนวก ๙ บัญชีคุมข้อมูลพิเศษ (NSDC-DG-209) ประกอบผนวก ค

๖.๒.๒.๑ (๗.๓) บัญชีควบคุมการขอความยินยอมในการเปิดเผยข้อมูลของเจ้าข้อมูลส่วนบุคคล โดยใช้แบบฟอร์ม ตามอนุผนวก ๑๐ การขอความยินยอมให้ข้อมูล (NSDC-DG-210) ประกอบผนวก ค

๖.๒.๒.๒ ขั้นตอนใช้

ในขั้นตอนใช้ มีผู้ที่มีส่วนได้ส่วนเสีย และแนวปฏิบัติในแต่ละประเด็นขององค์ประกอบการบริหารจัดการข้อมูลด้านความมั่นคงที่เกี่ยวข้อง ได้แก่ การจัดเก็บและการดำเนินงานต่อข้อมูลที่มีโครงสร้าง การบูรณาการและความสามารถในการทำงานร่วมกัน การบริหารจัดการเอกสารและเนื้อหาข้อมูลแบบกึ่งโครงสร้างและไม่มีโครงสร้าง การบริหารจัดการคลังข้อมูล ดาตาเลค และระบบรายงานอัจฉริยะ การบริหารจัดการความมั่นคงปลอดภัยและการรักษาความเป็นส่วนบุคคลของข้อมูล และการบริหารจัดการคุณภาพของข้อมูล ตามรูปที่ ๖.๔ ดังนี้



รูปที่ ๖.๔ ความสัมพันธ์การบริหารจัดการข้อมูลด้านใช้

๖.๒.๒.๒ (๑) ผู้ที่มีส่วนได้ส่วนเสียในขั้นตอนใช้ มีจำนวน ๖ กลุ่ม ประกอบด้วย : (๑) ส่วนงานบริหารจัดการข้อมูล (๒) ผู้ใช้งานข้อมูล (๓) ทีมบริหารจัดการข้อมูล (๔) ทีมบริกรข้อมูล กอ.รมน. (๕) เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล และ (๖) ศูนย์ดิจิทัลเพื่อความมั่นคง กอ.รมน.

๖.๒.๒.๒ (๒) ให้ กอ.รมน. จัดทำข้อตกลงหรือข้อตกลงร่วม กับหน่วยเจ้าของข้อมูลเกี่ยวกับการใช้งานข้อมูลในทุกขั้นตอนการปฏิบัติ ทั้งที่เป็นข้อมูลหลัก ข้อมูลอ้างอิง หรือกลุ่มข้อมูลอื่น ๆ ตามอนุผนวก ๔ การควบคุมคุณภาพข้อมูล (NSDC-DG-104) ประกอบผนวก ข ในประเด็นดังต่อไปนี้

๖.๒.๒.๒ (๒.๑) หัวข้อเรื่อง/ประเด็น ลักษณะและวัตถุประสงค์ในการใช้ข้อมูล ระยะเวลาในการใช้ และคำอธิบาย

๖.๒.๒.๒ (๒.๒) ประเภทของข้อมูล และเจ้าของข้อมูล โดยให้ระบุถึงความอ่อนไหวของข้อมูล ข้อมูลที่มีระดับชั้นความลับ ข้อมูลส่วนบุคคล หรือข้อมูลที่ส่งผลกระทบต่อความมั่นคงของชาติ

๖.๒.๒.๒ (๒.๓) ข้อกำหนดและสิทธิ ทั้งในระดับผู้ใช้งานข้อมูล ซึ่งรวมถึงเจ้าหน้าที่ของส่วนงานบริหารจัดการข้อมูล

๖.๒.๒.๒ (๒.๔) รายละเอียดเกี่ยวกับขอบเขตการใช้ของผู้ใช้งานข้อมูล รวมถึงการประมวลผล การรักษาความปลอดภัยข้อมูล การรักษาความลับ และการยินยอมให้ผู้ควบคุมข้อมูลส่วนบุคคล ตรวจสอบการใช้งานข้อมูล

๖.๒.๒.๒ (๓) ให้ส่วนงานบริหารจัดการข้อมูล ควบคุมความปลอดภัยและความเหมาะสมในการใช้งานข้อมูล และข้อมูลส่วนบุคคล โดยกำหนดมาตรการควบคุม ดังนี้

๖.๒.๒.๒ (๓.๑) กำหนดรายละเอียดข้อมูล เพื่อให้ผู้ใช้งานข้อมูลรับทราบถึงระดับในการรักษาความปลอดภัยที่เหมาะสม ตามสถานการณ์ และระดับผลประเมินความเสี่ยง

๖.๒.๒.๒ (๓.๒) กำหนดมาตรการและกำกับดูแลการรักษาความปลอดภัยและความเหมาะสมในการใช้งานข้อมูล ซึ่งรวมถึงการเชื่อมโยงและการประมวลผลข้อมูลด้วย

๖.๒.๒.๒ (๓.๓) ตรวจสอบร่วมกับศูนย์ดิจิทัลเพื่อความมั่นคง กอ.รมน. กรณีผู้ใช้งานข้อมูลมีความประสงค์ใช้งานอุปกรณ์เคลื่อนที่หรืออุปกรณ์ส่วนตัว ก่อนการอนุมัติการเข้าใช้งาน

๖.๒.๒.๒ (๓.๔) รักษาความปลอดภัยระหว่างการใช้งานข้อมูลให้เหมาะสมเพียงพอต่อระดับความเสี่ยงของข้อมูล และตลอดเวลาที่มีการใช้งานข้อมูล

๖.๒.๒.๒ (๓.๕) เพื่อควบคุมตรวจสอบการส่งคืน หรือทำลายทรัพย์สินข้อมูล โดยเฉพาะข้อมูลที่มีความเสี่ยงสูง โดยใช้ระบบบริหารจัดการทรัพย์สินข้อมูล

๖.๒.๒.๒ (๓.๖) จัดทำเอกสารควบคุมการเข้าถึงข้อมูล รวมทั้งกำกับให้ทีมบริหารจัดการข้อมูล ควบคุมและกำกับดูแลการเข้าถึงข้อมูลด้วย ตามอนุผนวก ๔ การจัดทำเอกสารควบคุมการเข้าถึงข้อมูล (NSDC-DG-304) ประกอบผนวก ง

๖.๒.๒.๒ (๔) ให้ส่วนงานบริหารจัดการข้อมูล กำหนดมาตรการและควบคุมการรักษาความปลอดภัยเพิ่มเติม กรณีข้อมูลที่มีความอ่อนไหว ข้อมูลที่ส่งผลกระทบต่อความมั่นคงของชาติ ข้อมูลที่อาจส่งผลกระทบต่อสิทธิและเสรีภาพของบุคคล หรือข้อมูลความลับทางราชการ ดังนี้

๖.๒.๒.๒ (๔.๑) ประสานศูนย์ดิจิทัลเพื่อความมั่นคง กอ.รมน. ร่วมตรวจสอบและประเมินสภาพแวดล้อมการรักษาความปลอดภัยของระบบเครือข่ายคอมพิวเตอร์ของผู้ใช้งานข้อมูล รวมทั้งในกรณีที่มีความประสงค์ใช้งานอุปกรณ์เคลื่อนที่หรืออุปกรณ์ส่วนตัว เพื่อขออนุมัติตามสายงานด้านการข่าว กอ.รมน. และนำผลไปใช้ประกอบในการพิจารณาให้สิทธิในการเข้าถึงข้อมูล

๖.๒.๒.๒ (๔.๒) ก่อนการอนุมัติสิทธิในการเข้าถึงข้อมูลให้กับผู้ใช้งานข้อมูล ต้องตรวจสอบรายละเอียดตามแนวทางหรือมาตรฐานที่คณะกรรมธรรมาภิบาลข้อมูล กอ.รมน. เห็นชอบ ทั้งนี้ต้องระงับสิทธิการเข้าถึงข้อมูลของผู้ใช้งาน เมื่อตรวจพบการไม่ปฏิบัติตามแนวทางหรือมาตรฐานที่กำหนด หรือมีเหตุอันควร ในทันที

๖.๒.๒.๒ (๔.๓) ให้เข้ารหัสข้อมูลตลอดระยะเวลาที่มีการใช้งานหรือดำเนินการใด ๆ กับข้อมูล โดยตรวจสอบการดำเนินการตามมาตรการการเข้ารหัสข้อมูลที่กำหนด ตามแนวทางหรือมาตรฐานที่คณะกรรมธรรมาภิบาลข้อมูล กอ.รมน. เห็นชอบ

๖.๒.๒.๒ (๔.๔) ทั้งนี้ ส่วนงานบริหารจัดการข้อมูล ทีมบริหารจัดการข้อมูล และผู้ใช้ข้อมูลต้องพร้อมรับการตรวจสอบการใช้ข้อมูลดังกล่าวจากทีมบริกรข้อมูล กอ.รมน. และเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล เมื่อได้รับการประสาน

๖.๒.๒.๒ (๕) ให้ทีมบริหารจัดการข้อมูลและผู้ใช้งานข้อมูล เลือกใช้งานข้อมูลที่มีคุณภาพ ถูกต้อง ครบถ้วน สอดคล้องต้องกัน เป็นปัจจุบัน และตรงตามความต้องการหรือวัตถุประสงค์การดำเนินการที่แท้จริง โดยเข้าใช้งานข้อมูลตามวิธีการ เครื่องมือ และสภาพแวดล้อมการเข้าใช้งานข้อมูล ตามที่ กอ.รมน. โดยส่วนงานบริหารจัดการข้อมูลกำหนด โดยบันทึกประวัติการเข้าใช้งานข้อมูล โดยใช้แบบฟอร์มตามอนุผนวก ๑๑ การบันทึกประวัติการเข้าใช้งานข้อมูล (NSDC-DG-211) ประกอบผนวก ค ดังนี้

๖.๒.๒.๒ (๕.๑) ชุดข้อมูลที่ใช้งาน และรายละเอียดที่บ่งบอกถึงการอนุญาตให้ผู้ใช้งานข้อมูลสามารถเข้าถึงชุดข้อมูลได้ เช่น เอกสารคำขอ หรือข้อตกลงฯ ที่กำหนดให้เข้าถึงชุดข้อมูล

๖.๒.๒.๒ (๕.๒) รายละเอียดผู้ใช้งานข้อมูล เช่น บัญชีผู้ใช้งาน

๖.๒.๒.๒ (๕.๓) วันเวลาที่ใช้งานข้อมูล รวมถึงรายละเอียดการใช้งานข้อมูล เป็นต้น

๖.๒.๒.๒ (๖) ให้ส่วนงานบริหารจัดการข้อมูล ควบคุมและตรวจสอบการดำเนินการของผู้ใช้งานข้อมูล รวมทั้งตรวจสอบบันทึกประวัติการใช้งานข้อมูล ตามวงรอบภายในระยะเวลาที่เหมาะสมกับระดับความเสี่ยงของข้อมูล เพื่อเป็นมาตรการควบคุมในการรักษาความปลอดภัย และตรวจสอบควบคุมการเข้าถึงข้อมูล โดยจัดเก็บเป็นหลักฐานในการประเมินผล ตามอนุผนวก ๑๒ การบันทึกการตรวจสอบประวัติการเข้าใช้งานข้อมูล (NSDC-DG-212) ประกอบผนวก ค ดังนี้

๖.๒.๒.๒ (๖.๑) วัน เวลาในการประเมิน ผู้ประเมิน ผู้รับการประเมิน และประเภทของข้อมูลที่มีการนำไปใช้งาน

๖.๒.๒.๒ (๖.๒) ข้อมูลนโยบายด้านการรักษาความปลอดภัยข้อมูลของผู้รับการประเมิน หรือใบรับรองมาตรฐานด้านการรักษาความปลอดภัย

๖.๒.๒.๒ (๖.๓) ข้อมูล และรายละเอียดข้อมูล ได้แก่ ปริมาณ ประเภทและคุณภาพ ที่ดำเนินการโดยผู้ใช้งานข้อมูล รวมทั้งเหตุผลในการใช้งาน

๖.๒.๒.๒ (๖.๔) ตรวจสอบการควบคุมด้านการรักษาความปลอดภัยข้อมูล ที่เหมาะสมเพียงพอต่อระดับความเสี่ยงของข้อมูล

๖.๒.๒.๒ (๖.๕) ตรวจสอบการแบ่งปันข้อมูล หรือการให้บุคคลที่สามดำเนินการต่อข้อมูล (ถ้ามี) ให้เป็นไปตามข้อตกลงในการใช้ข้อมูล

๖.๒.๒.๒ (๖.๖) ทั้งนี้ ให้จัดทำบันทึกประวัติ ข้อพิจารณา คำแนะนำเพิ่มเติม เพื่อนำไปใช้ประกอบการตรวจสอบครั้งต่อ ๆ ไปด้วย

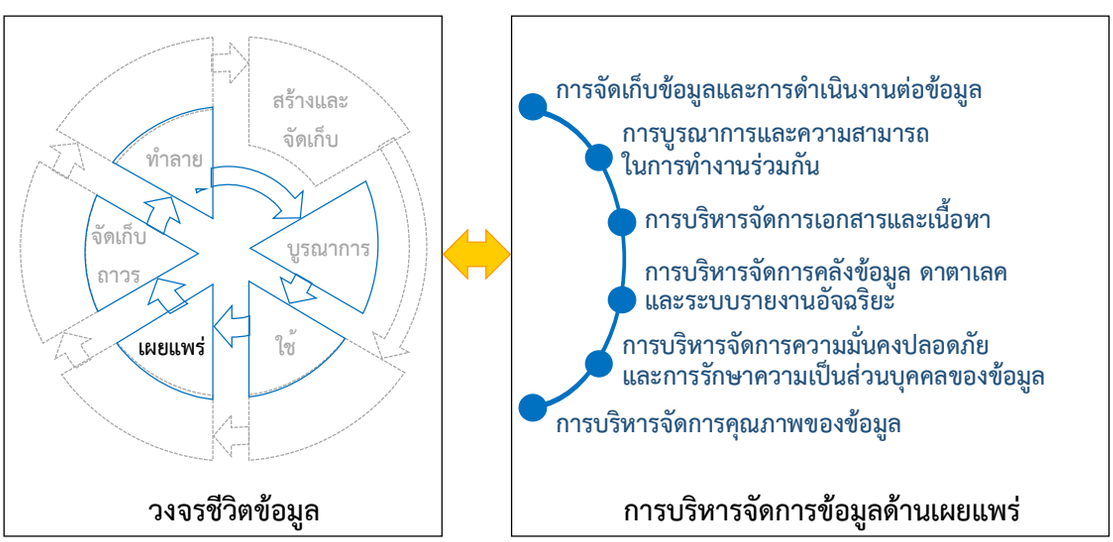
๖.๒.๒.๒ (๗) ให้ส่วนงานบริหารจัดการข้อมูล ตรวจสอบสภาพแวดล้อมที่เกี่ยวกับการใช้งานข้อมูล เช่น การใช้เครือข่ายและอุปกรณ์ในการเข้าถึงข้อมูลของผู้ใช้งานข้อมูล ในทุกขั้นตอน ทั้งนี้หากตรวจพบการปฏิบัติที่ไม่เป็นไปตามข้อกำหนด ระเบียบ กฎหมาย หรือไม่ได้รับอนุญาต ให้ถือเป็นการละเมิด

การรักษาความมั่นคงปลอดภัยข้อมูล และมีสิทธิในการระงับการเข้าถึงข้อมูลของผู้ใช้งานทันที และบันทึกในแบบฟอร์ม ตามอนุผนวก ๑๓ การบันทึกการระงับการเข้าถึงข้อมูล (NSDC-DG-213) ประกอบผนวก ค

๖.๒.๒.๒ (๘) ให้ส่วนงานบริหารจัดการข้อมูล สนับสนุนสถาปัตยกรรมข้อมูลแบบจำลองข้อมูล รวมทั้งเมทาดาตา (ระดับบูรณาการ) ให้กับส่วนงาน หน่วยงาน ผู้ใช้ข้อมูล หรือผู้ที่เกี่ยวข้อง เพื่ออำนวยความสะดวกต่อการสืบค้น ค้นหา และเข้าถึงข้อมูลได้โดยสะดวก

๖.๒.๒.๓ ขั้นตอนเผยแพร่

ในขั้นตอนเผยแพร่ มีผู้ที่มีส่วนได้ส่วนเสีย และแนวปฏิบัติในแต่ละประเด็นขององค์ประกอบการบริหารจัดการข้อมูลด้านความมั่นคงที่เกี่ยวข้อง ได้แก่ การจัดเก็บและการดำเนินงานต่อข้อมูลที่มีโครงสร้าง การบูรณาการและความสามารถในการทำงานร่วมกัน การบริหารจัดการเอกสารและเนื้อหา ข้อมูลแบบกึ่งโครงสร้างและแบบไม่มีโครงสร้าง การบริหารจัดการคลังข้อมูล ดาตาเลค และระบบรายงานอัจฉริยะ การบริหารจัดการความมั่นคงปลอดภัยและการรักษาความเป็นส่วนบุคคลของข้อมูล และการบริหารจัดการคุณภาพของข้อมูล ตามรูปที่ ๖.๕ ดังนี้



รูปที่ ๖.๕ ความสัมพันธ์การบริหารจัดการข้อมูลด้านเผยแพร่

๖.๒.๒.๓ (๑) ผู้ที่มีส่วนได้ส่วนเสียในขั้นตอนเผยแพร่ มีจำนวน ๗ กลุ่ม ประกอบด้วย : (๑) ส่วนงานบริหารจัดการข้อมูล (๒) ทีมบริหารจัดการข้อมูล (๓) ผู้ใช้งานข้อมูล (๔) เจ้าของข้อมูลส่วนบุคคล (๕) ทีมบริกรข้อมูล กอ.รมน. (๖) เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล และ (๗) ศูนย์ดิจิทัลเพื่อความมั่นคง กอ.รมน.

๖.๒.๒.๓ (๒) ให้ส่วนงานบริหารจัดการข้อมูล วางแผน กำหนดแนวทาง บริหารจัดการตรวจสอบคุณภาพข้อมูล และดำเนินการเผยแพร่ข้อมูล ตามแนวทางหรือมาตรฐานที่คณะกรรมการธรรมาภิบาลข้อมูล กอ.รมน. กำหนด โดยมีการรักษาความมั่นคงปลอดภัยและอำนวยความสะดวกในการเผยแพร่และเปิดเผยข้อมูล อย่างเป็นระบบ ดังนี้

๖.๒.๒.๓ (๒.๑) สำรวจความต้องการ ตรวจสอบและคัดเลือกข้อมูลที่จะเผยแพร่ รวมทั้งตรวจสอบและปรับปรุงคุณภาพข้อมูล เพื่อจัดทำรายการบัญชีข้อมูลเผยแพร่ ที่ระบุประเภทชุดข้อมูล และแนวทางการเผยแพร่ โดยใช้แบบฟอร์ม ตามอนุผนวก ๑๔ รายการบัญชีข้อมูลเผยแพร่ (NSDC-DG-214) ประกอบผนวก ค

๖.๒.๒.๓ (๒.๒) ทวนสอบรายการบัญชีข้อมูลเผยแพร่ ต้องไม่มีชุดข้อมูลที่ขัดต่อกฎหมาย ระเบียบ ข้อบังคับ คำสั่ง นโยบาย แนวปฏิบัติ ความมั่นคงของชาติ ความลับทางราชการ หรือก้าวล่วงความเป็นส่วนตัวของบุคคล ทั้งนี้กรณีการเผยแพร่ข้อมูลส่วนบุคคล ต้องได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคล หรืออยู่ในขอบเขตที่กฎหมายกำหนด เท่านั้น

๖.๒.๒.๓ (๒.๓) เตรียมข้อมูลให้อยู่ในรูปแบบที่ง่ายต่อการเผยแพร่และเป็นมาตรฐานสากล รวมทั้งเมทาดาตาของข้อมูล

๖.๒.๒.๓ (๒.๔) กำหนดมาตรการในการรักษาความปลอดภัยข้อมูล การเข้าถึง การแก้ไขเปลี่ยนแปลงข้อมูล เป้าหมายการเผยแพร่ข้อมูล และการป้องกันข้อมูลที่สามารถระบุตัวบุคคลได้แก่ การพลางหรือปกปิดข้อมูลบางส่วนเพื่อจำกัดการเข้าถึงข้อมูลทั้งหมด หรือการทำข้อมูลนิรนาม

๖.๒.๒.๓ (๒.๕) กำหนดช่องทางเผยแพร่ชุดข้อมูล ผ่านระบบสื่อสารข้อมูลของ กอ.รมน. รวมทั้งหน่วยงานของรัฐ ที่มีการรักษาความมั่นคงปลอดภัยไซเบอร์ เป็นหลัก

๖.๒.๒.๓ (๓) ในกรณีเผยแพร่ข้อมูลภายใน กอ.รมน. หรือระหว่างหน่วยงานให้ส่วนงานบริหารจัดการข้อมูล จัดทำข้อตกลงร่วมเกี่ยวกับการเผยแพร่ข้อมูล ตามอนุผนวก ๕ ข้อตกลงร่วมเกี่ยวกับการเผยแพร่ข้อมูล (NSDC-DG-105) ประกอบผนวก ข ในประเด็นดังต่อไปนี้

๖.๒.๒.๓ (๓.๑) หัวข้อเรื่อง/ประเด็น ลักษณะและวัตถุประสงค์ในการเผยแพร่ ระยะเวลาในการเผยแพร่ และการทำลายข้อมูล และคำอธิบาย

๖.๒.๒.๓ (๓.๒) ประเภทของข้อมูล และเจ้าของข้อมูล โดยให้ตรวจสอบและระบุถึงความอ่อนไหวของข้อมูล ข้อมูลที่มีระดับชั้นความลับ ข้อมูลส่วนบุคคล หรือข้อมูลที่ส่งผลกระทบต่อความมั่นคงของชาติ

๖.๒.๒.๓ (๓.๓) วิธีการ ข้อกำหนด สิทธิ รวมทั้งการอำนวยความสะดวกให้กับผู้ใช้งานข้อมูล

๖.๒.๒.๓ (๓.๔) รายละเอียดเกี่ยวกับขอบเขตการเข้าถึงข้อมูล รวมถึงการประมวลผล การรักษาความปลอดภัยข้อมูล การรักษาความลับ และการยินยอมให้ผู้ควบคุมข้อมูลส่วนบุคคลตรวจสอบการเผยแพร่ข้อมูล

๖.๒.๒.๓ (๓.๕) มอบหมายให้ทีมบริหารจัดการข้อมูล บันทึกประวัติการเผยแพร่ข้อมูล ตามอนุผนวก ๑๕ การบันทึกประวัติการเผยแพร่ข้อมูล (NSDC-DG-215) ประกอบผนวก ค สำหรับจัดทำเอกสารควบคุมหรือระบบบริหารจัดการทรัพย์สินข้อมูล เพื่อควบคุมการแก้ไข ปรับปรุง ตรวจสอบการส่งคืน หรือทำลายทรัพย์สินข้อมูลที่เผยแพร่ โดยเฉพาะข้อมูลที่มีความเสี่ยงสูง อย่างเป็นระบบ

๖.๒.๒.๓ (๔) ในกรณีเผยแพร่ข้อมูลในลักษณะเปิดเผยข้อมูลออกสู่สาธารณะ ให้ส่วนงานบริหารจัดการข้อมูล กำหนดมาตรการ อำนวยความสะดวกในการเผยแพร่ข้อมูล รวมทั้งควบคุม

ความปลอดภัยอย่างเหมาะสม ตามอนุผนวก ๖ มาตรการการเผยแพร่ข้อมูลออกสู่สาธารณะ (NSDC-DG-106) ประกอบผนวก ข ดังนี้

๖.๒.๒.๓ (๔.๑) รายละเอียดข้อมูลที่ทำการเผยแพร่ให้มีความชัดเจน รวมทั้งความปลอดภัยและระดับความเสี่ยง

๖.๒.๒.๓ (๔.๒) มาตรการและกำกับดูแลการรักษาความปลอดภัยและความเหมาะสมในการเผยแพร่ข้อมูล ซึ่งรวมถึงวิธีการ ช่องทางเผยแพร่ข้อมูลด้วย

๖.๒.๒.๓ (๔.๓) รักษาความปลอดภัยระหว่างการเผยแพร่ข้อมูลให้เหมาะสมเพียงพอต่อระดับความเสี่ยงของข้อมูล

๖.๒.๒.๓ (๔.๔) จัดทำเอกสารควบคุมการเผยแพร่ รวมทั้งกำกับให้เจ้าหน้าที่ควบคุมข้อมูล กำกับดูแลการเผยแพร่ข้อมูลด้วย

๖.๒.๒.๓ (๕) ให้ส่วนงานบริหารจัดการข้อมูล กำหนดมาตรการควบคุมและการรักษาความปลอดภัยเพิ่มเติม กรณีข้อมูลที่มีความอ่อนไหว ข้อมูลที่ส่งผลกระทบต่อความมั่นคงของชาติ ข้อมูลที่อาจส่งผลกระทบต่อสิทธิและเสรีภาพของบุคคล หรือข้อมูลความลับทางราชการ ดังนี้

๖.๒.๒.๓ (๕.๑) ประสานศูนย์ดิจิทัลเพื่อความมั่นคง กอ.รมน. ร่วมตรวจสอบและประเมินสภาพแวดล้อมการรักษาความปลอดภัยของระบบเครือข่ายคอมพิวเตอร์ของผู้ใช้งานข้อมูล เพื่อนำผลไปใช้ประกอบในการพิจารณาการกำหนดสิทธิ

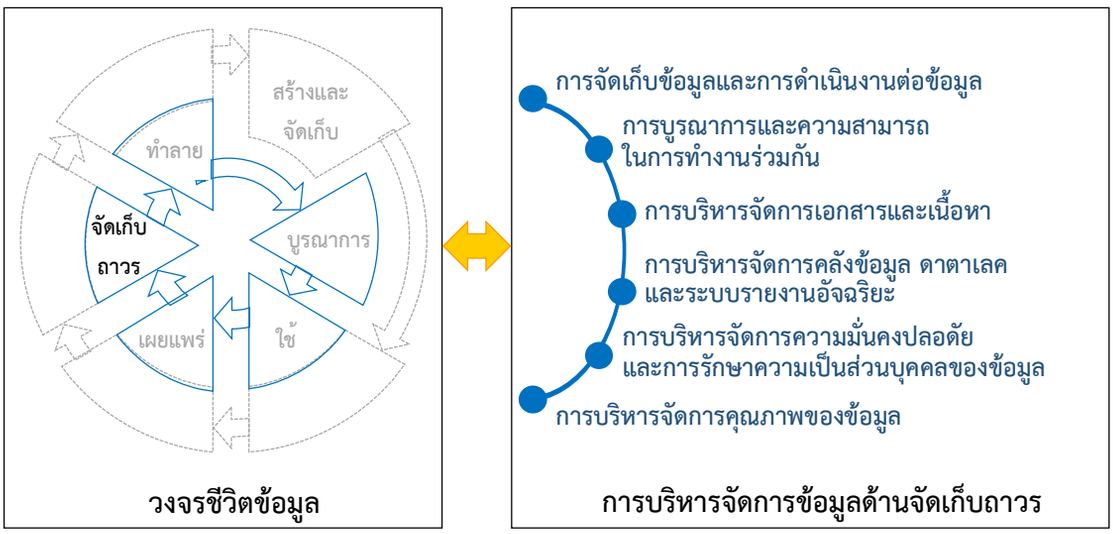
๖.๒.๒.๓ (๕.๒) ก่อนการอนุมัติสิทธิในการเข้าถึงข้อมูลให้กับผู้ใช้งานข้อมูล ต้องตรวจสอบรายละเอียดตามแนวทางหรือมาตรฐานที่คณะกรรมการธรรมาภิบาลข้อมูล กอ.รมน. กำหนด ทั้งนี้ต้องระงับสิทธิการเข้าถึงข้อมูลของผู้ใช้งาน เมื่อตรวจพบการไม่ปฏิบัติตามแนวทางหรือมาตรฐานที่กำหนด หรือมีเหตุอันควร ในทันที

๖.๒.๒.๓ (๕.๓) ให้เข้ารหัสข้อมูลตลอดระยะเวลาระหว่างการเผยแพร่ข้อมูล โดยตรวจสอบการดำเนินการตามมาตรการการเข้ารหัสข้อมูลที่กำหนด ตามแนวทางหรือมาตรฐานที่คณะกรรมธรรมาภิบาลข้อมูล กอ.รมน. เห็นชอบ ตามอนุผนวก ๗ การเข้ารหัสข้อมูล (NSDC-DG-107) ประกอบผนวก ข

๖.๒.๒.๓ (๕.๔) ทั้งนี้ ส่วนงานบริหารจัดการข้อมูล ทีมบริหารจัดการข้อมูล และผู้ใช้งานข้อมูลต้องพร้อมรับการตรวจสอบการเผยแพร่ข้อมูลดังกล่าวจากทีมบริกรข้อมูล กอ.รมน. และเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล เมื่อได้รับการประสาน

๖.๒.๒.๔ ขั้นตอนจัดเก็บถาวร

ในขั้นตอนจัดเก็บถาวร มีผู้ที่มีส่วนได้ส่วนเสีย และแนวปฏิบัติในแต่ละประเด็นขององค์ประกอบการบริหารจัดการข้อมูลด้านความมั่นคงที่เกี่ยวข้อง ได้แก่ การบริหารจัดการคลังข้อมูลและดาตาเลค ที่ต้องกำหนดแนวทางการดำเนินการต่อข้อมูลที่ได้จัดเก็บไว้เกินระยะเวลาที่กำหนดตามขั้นตอนสร้างและจัดเก็บ รวมถึงข้อมูลที่ไม่มีการใช้งานแล้ว ด้วยวิธีการโอนย้ายข้อมูลเข้าไปจัดเก็บในพื้นที่จัดเก็บถาวร แต่ยังคงสามารถนำกลับมาใช้งานได้อีกเมื่อต้องการ ผ่านการบริหารจัดการความมั่นคงปลอดภัยและการรักษาความเป็นส่วนบุคคลของข้อมูล และการบริหารจัดการคุณภาพของข้อมูล อย่างเป็นระบบ ตามรูปที่ ๖.๖ ดังนี้



รูปที่ ๖.๖ ความสัมพันธ์การบริหารจัดการข้อมูลด้านจัดเก็บถาวร

๖.๒.๒.๔ (๑) ผู้ที่มีส่วนได้ส่วนเสียในขั้นตอนจัดเก็บถาวร มีจำนวน ๙ กลุ่ม ประกอบด้วย : (๑) ส่วนงานบริหารจัดการข้อมูล (๒) ทีมบริหารจัดการข้อมูล (๓) ส่วนงานเจ้าของข้อมูล (๔) หน่วยงานเจ้าของข้อมูล (๕) ผู้ใช้งานข้อมูล (๖) เจ้าของข้อมูลส่วนบุคคล (๗) ทีมบริกรข้อมูล กอ.รมน. (๘) เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล และ (๙) ศูนย์ดิจิทัลเพื่อความมั่นคง กอ.รมน.

๖.๒.๒.๔ (๒) ให้ส่วนงานบริหารจัดการข้อมูล วางแผน กำหนดแนวทาง บริหารจัดการและดำเนินการเพื่อย้ายข้อมูลไปจัดเก็บถาวร ตามแนวทางหรือมาตรฐานที่คณะกรรมการธรรมาภิบาลข้อมูล กอ.รมน. กำหนด โดยมีการรักษาความมั่นคงปลอดภัย อย่างเป็นระบบ ดังนี้

๖.๒.๒.๔ (๒.๑) กำหนดวิธีการ ระบบ ขั้นตอน ช่วงเวลาในการจัดเก็บข้อมูลถาวร ทั้งนี้ให้ทดสอบวิธีการ ระบบ ขั้นตอน ในการจัดเก็บข้อมูลถาวรอย่างน้อยปีละ ๑ ครั้ง รวมทั้งก่อนการนำข้อมูลที่ได้จัดเก็บถาวร ต้องตรวจสอบคุณภาพ ความถูกต้องครบถ้วนสมบูรณ์ของข้อมูลที่ก่อนทุกครั้ง

๖.๒.๒.๔ (๒.๒) จัดทำเอกสารควบคุมประวัติการจัดเก็บข้อมูลถาวร หรือระบบบริหารจัดการทรัพย์สินข้อมูลถาวร เพื่อควบคุมการโอนย้าย ห้วงเวลา การแก้ไขปรับปรุง การเรียกใช้งาน การโอนข้อมูลกลับ และการทำลายทรัพย์สินข้อมูลถาวร โดยเฉพาะข้อมูลที่มีความเสี่ยงสูงอย่างเป็นระบบ โดยใช้แบบฟอร์ม ตามอนุผนวก ๑๖ บัญชีคุมข้อมูลถาวร (NSDC-DG-216) ประกอบผนวก ค

๖.๒.๒.๔ (๒.๓) กำหนดมาตรการในการรักษาความปลอดภัยข้อมูลที่ทำการย้าย การลบข้อมูลเดิม การจัดเก็บถาวร รวมทั้งการรักษาความมั่นคงปลอดภัยไซเบอร์

๖.๒.๒.๔ (๒.๔) กำหนดเครื่องมือและพื้นที่ที่ใช้ในการจัดเก็บข้อมูลถาวร

๖.๒.๒.๔ (๓) ให้ส่วนงานบริหารจัดการข้อมูล กำหนดมาตรการควบคุมและการรักษาความปลอดภัยเพิ่มเติม กรณีข้อมูลที่มีความอ่อนไหว ข้อมูลที่ส่งผลกระทบต่อความมั่นคงของชาติ ข้อมูลที่อาจส่งผลกระทบต่อสิทธิและเสรีภาพของบุคคล หรือข้อมูลความลับทางราชการ ดังนี้

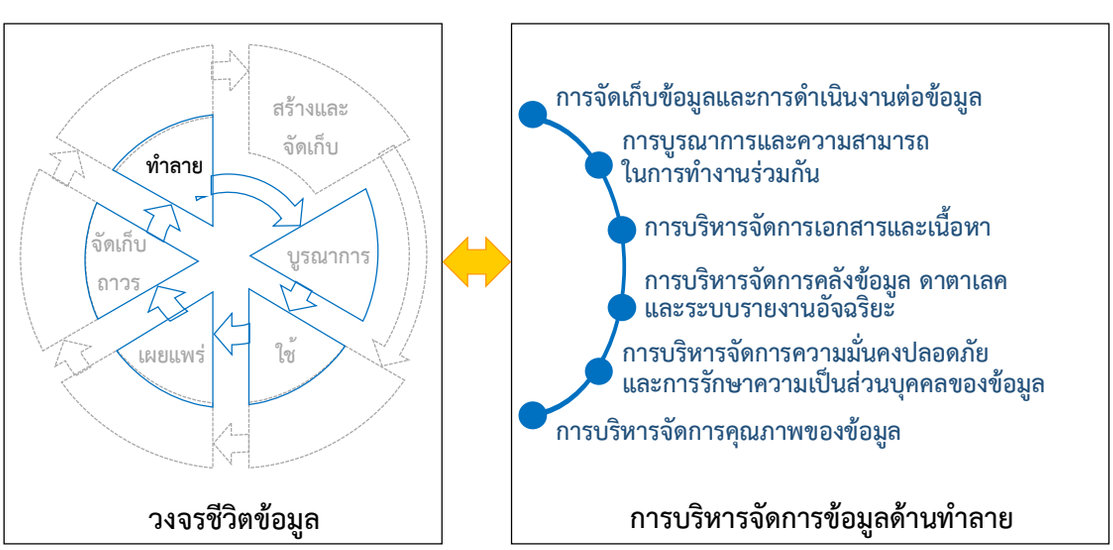
๖.๒.๒.๔ (๓.๑) ประสานศูนย์ดิจิทัลเพื่อความมั่นคง กอ.รมน. ร่วมตรวจสอบและประเมินสภาพแวดล้อมการรักษาความปลอดภัยของระบบเครือข่ายคอมพิวเตอร์สำหรับการจัดเก็บถาวร

๖.๒.๒.๔ (๓.๒) ให้เข้ารหัสข้อมูลตลอดระยะเวลาการจัดเก็บถาวร โดยตรวจสอบการดำเนินการตามมาตรการการเข้ารหัสข้อมูลที่กำหนด ตามแนวทางหรือมาตรฐานที่คณะกรรมการธรรมาภิบาลข้อมูล เห็นชอบ

๖.๒.๒.๔ (๔) ทั้งนี้ ส่วนงานบริหารจัดการข้อมูลและทีมบริหารจัดการข้อมูล ต้องพร้อมรับการตรวจสอบการจัดเก็บข้อมูลถาวรจากทีมบริกรข้อมูล กอ.รมน. และเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล เมื่อได้รับการประสาน

๖.๒.๒.๕ ขั้นตอนทำลาย

ในขั้นตอนทำลาย มีผู้ที่มีส่วนได้ส่วนเสีย และแนวปฏิบัติในแต่ละประเด็นขององค์ประกอบการบริหารจัดการข้อมูลด้านความมั่นคงที่เกี่ยวข้อง ได้แก่ การจัดเก็บและการดำเนินงานต่อข้อมูล การบริหารจัดการเอกสารและเนื้อหาข้อมูล การบริหารจัดการคลังข้อมูลและดาตาเลค ของหน่วยงาน ซึ่งมีการจัดเก็บการจัดเก็บถาวรเป็นระยะเวลานานหรือเกินกว่าระยะที่กำหนด หรือมีการร้องขอให้ทำลายข้อมูล ภายใต้การบริหารจัดการความมั่นคงปลอดภัยและการรักษาความเป็นส่วนบุคคลของข้อมูล ตามรูปที่ ๖.๗ ดังนี้



รูปที่ ๖.๗ ความสัมพันธ์การบริหารจัดการข้อมูลด้านทำลาย

๖.๒.๒.๕ (๑) ผู้ที่มีส่วนได้ส่วนเสียในขั้นตอนทำลาย มีจำนวน ๙ กลุ่ม ประกอบด้วย : (๑) หัวหน้าส่วนงานบริหารจัดการข้อมูล (๒) ทีมบริหารจัดการข้อมูล (๓) ส่วนงานบริหารจัดการข้อมูล (๔) ส่วนงานเจ้าของข้อมูล (๕) หน่วยงานเจ้าของข้อมูล (๖) เจ้าของข้อมูลส่วนบุคคล (๗) ทีมบริกรข้อมูล กอ.รมน. (๘) เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล และ (๙) คณะกรรมการทำลายข้อมูลประจำปี

๖.๒.๒.๕ (๒) ให้ส่วนงานบริหารจัดการข้อมูล ปฏิบัติให้เป็นไปตามกรอบระเบียบกฎหมายที่เกี่ยวข้อง ได้แก่ ระเบียบสำนักนายกรัฐมนตรี ว่าด้วยงานสารบรรณ พ.ศ. ๒๕๒๖ และที่แก้ไขเพิ่มเติม โดยมีรายละเอียดการดำเนินการเกี่ยวกับข้อมูล (เพิ่มเติม) ในข้อ ๖.๒.๒.๕ (๓) - ๖.๒.๒.๕ (๖)

๖.๒.๒.๕ (๓) ให้ส่วนงานบริหารจัดการข้อมูล ตรวจสอบและจัดทำบัญชีขอทำลายข้อมูลที่ครบอายุการจัดเก็บตามที่ระบุในข้อ ๖.๒.๒.๑ (๕) และข้อ ๖.๒.๒.๔ (๒.๑) หรือข้อมูลที่เก็บไว้ไม่เกิดประโยชน์หรือข้อมูลไม่มีการใช้งานใด ๆ ภายใน ๖๐ วัน หลังจากวันสิ้นปีปฏิทิน ทั้งนี้ให้ตรวจสอบผลกระทบจากการทำลายข้อมูลใด ๆ ต้องไม่ส่งผลกระทบต่อคุณภาพของชุดข้อมูลที่ยังจัดเก็บและใช้งานอยู่ โดยใช้แบบฟอร์ม ตามอนุผนวก ๑๗ บัญชีขอทำลายข้อมูล (NSDC-DG-217) ประกอบผนวก ค

๖.๒.๒.๕ (๔) ให้ส่วนงานบริหารจัดการข้อมูล แต่งตั้งคณะกรรมการทำลายข้อมูลประจำปี โดยมี นายทหารสัญญาบัตร หรือข้าราชการพลเรือนระดับ ๓ หรือเทียบเท่าขึ้นไป จำนวน ๓ คนขึ้นไป เป็นองค์ประกอบคณะกรรมการฯ ดำเนินการดังนี้

๖.๒.๒.๕ (๔.๑) ทวนสอบบัญชีขอทำลายข้อมูล และให้ข้อเสนอแนะกรณีเห็นสมควรทำลาย หรือขยายระยะเวลาการจัดเก็บข้อมูล ให้หัวหน้าส่วนงานบริหารจัดการข้อมูล พิจารณาอนุมัติ ทั้งนี้ในกรณีเสนอให้ขยายระยะเวลาการจัดเก็บ ให้ระบุห้วงระยะเวลาที่ขยายออกไปให้ชัดเจนด้วย โดยใช้แบบฟอร์ม ตามอนุผนวก ๑๘ บัญชีการทวนสอบขอทำลายข้อมูล (NSDC-DG-218) ประกอบผนวก ค

๖.๒.๒.๕ (๔.๒) ควบคุมกำกับดูแลการทำลายข้อมูลที่ได้รับอนุมัติให้ทำลาย จากระบบจัดเก็บข้อมูลทั้งหมด และเมื่อทำลายแล้วให้บันทึกรายงานให้หัวหน้าส่วนงานบริหารจัดการข้อมูลทราบ รวมทั้งแจ้งให้ส่วนงานหรือหน่วยงานเจ้าของข้อมูลทราบ

๖.๒.๒.๕ (๕) ให้บันทึกสถานการณ์ทำลายข้อมูล ในเอกสารควบคุมประวัติการจัดเก็บข้อมูล/ข้อมูลถาวร หรือจากระบบบริหารจัดการทรัพย์สินข้อมูล/ข้อมูลถาวร ของส่วนงานบริหารจัดการข้อมูล เพื่อให้สามารถตรวจสอบประวัติได้ในภายหลัง โดยใช้แบบฟอร์ม ตามอนุผนวก ๑๙ บัญชีคุมข้อมูลทำลาย (NSDC-DG-219) ประกอบผนวก ค

๖.๒.๒.๕ (๖) ทั้งนี้ ในกรณีที่การเก็บข้อมูลที่มีระดับชั้นความลับที่สุด และอาจเสี่ยงต่อการรั่วไหลอันจะเกิดอันตรายแก่ประโยชน์แห่งรัฐ หรือข้อมูลที่ส่งผลกระทบต่อความมั่นคงของชาติ ข้อมูลที่อาจส่งผลกระทบต่อสิทธิและเสรีภาพของบุคคล ให้ส่วนงานบริหารจัดการข้อมูล พิจารณาสั่งทำลายได้ หากเห็นว่ามีความจำเป็นอย่างยิ่ง โดยดำเนินการตามขั้นตอนในข้อ ๖.๒.๒.๕ (๔) และข้อ ๖.๒.๒.๕ (๕)

๖.๒.๒.๕ (๗) ทั้งนี้ ส่วนงานบริหารจัดการข้อมูลและทีมบริหารจัดการข้อมูล ต้องพร้อมรับการตรวจสอบการทำลายข้อมูลจากทีมบริกรข้อมูล กอ.รมน. และเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล เมื่อได้รับการประสาน

๖.๓ แนวปฏิบัติในการขับเคลื่อนการบริหารจัดการความเสี่ยงระดับบูรณาการ

แนวปฏิบัติในการขับเคลื่อนการบริหารจัดการความเสี่ยง จะต้องดำเนินการให้สอดคล้องกับระดับความเสี่ยงของข้อมูล โดยกำหนดระดับความเสี่ยงและความร้ายแรงของผลกระทบ (Impact Levels) แบ่งเป็น ระดับต่ำ ระดับกลาง และระดับสูง ซึ่งมีความเกี่ยวข้องกับคุณภาพข้อมูลในทุกขั้นตอนของวงจรชีวิตข้อมูล โดยผู้ที่มีส่วนได้ส่วนเสีย พึงตระหนักและเตรียมการล่วงหน้า ให้สามารถปฏิบัติได้ในทันทีที่เกิดเหตุการณ์ ทั้งนี้ ได้กำหนดปัจจัยที่มีอิทธิพลต่อความเสี่ยง ได้แก่ ความสำคัญของข้อมูล ระดับชั้นความลับ ความเป็นส่วนบุคคล ปริมาณ

หรือขนาดของข้อมูล จำนวนผู้ใช้งานและจำนวนกิจกรรมที่ใช้ข้อมูล ความอ่อนไหวของข้อมูล และผลกระทบต่อความมั่นคง เจ้าของข้อมูล หน่วยงานของรัฐหรือภาคเอกชนที่เกี่ยวข้อง รัฐบาล และประเทศ เป็นต้น

๖.๓.๑ ให้ส่วนงานบริหารจัดการข้อมูล ประเมินความเสี่ยงของข้อมูล เพื่อรวบรวมปัญหา ข้อบกพร่อง ช่องโหว่ ฯลฯ ที่อาจเกิดขึ้นกับข้อมูลในแต่ละขั้นตอนบนวงจรชีวิตข้อมูล ทั้งที่เป็นแบบมีเจตนาและไม่มีเจตนา เพื่อนำไปใช้ประกอบการกำหนดมาตรการควบคุมความเสี่ยงและป้องกันเหตุการณ์ที่อาจมีผลกระทบต่อข้อมูล โดยใช้แบบฟอร์ม ตามอนุผนวก ๒๐ การประเมินความเสี่ยง (NSDC-DG-220) ประกอบผนวก ค ทั้งนี้ให้ทบทวนกระบวนการประเมินความเสี่ยง อย่างน้อยปีละ ๑ ครั้ง ในประเด็นดังต่อไปนี้

๖.๓.๑.๑ ระบุปัจจัยที่มีอิทธิพลต่อความเสี่ยง ต้นเหตุ หรือบ่อเกิดแห่งเหตุการณ์ของความเสี่ยง เช่น การเข้าถึงระบบโดยมิชอบ หรือการดัดแปลงข้อมูล เป็นต้น

๖.๓.๑.๒ ระบุระดับความน่าจะเป็นของเหตุการณ์ที่ทำให้เกิดความเสี่ยง เช่น โอกาสเกิดเหตุการณ์สูง กลาง หรือต่ำ

๖.๓.๑.๓ กำหนดระดับความเสี่ยงและความร้ายแรงของผลกระทบ

๖.๓.๑.๔ ระบุผลกระทบที่เกิดจากความเสี่ยง เช่น ทำให้เกิดความเสียหายแก่ชื่อเสียง ทำให้สูญเสียความลับ หรือทำให้ข้อมูลสามารถระบุความเป็นส่วนบุคคล เป็นต้น

๖.๓.๑.๕ กำหนดมาตรการเพื่อลดความเสี่ยง เช่น การเพิ่มมาตรการทางเทคโนโลยีเพื่อความปลอดภัย การฝึกอบรมบุคลากรให้สามารถประเมินความเสี่ยงและจัดการความเสี่ยงได้ และการแฝงข้อมูลหรือทำให้ข้อมูลไม่สามารถระบุตัวตนได้

๖.๓.๒ ให้ส่วนงานบริหารจัดการข้อมูล กำหนดขั้นตอนและแนวปฏิบัติเพื่อประเมินความพร้อมของการธรรมาภิบาลข้อมูลในแต่ละปัจจัยที่มีอิทธิพลต่อความเสี่ยง อย่างเป็นวงรอบ ตามอนุผนวก ๘ การประเมินความพร้อมการธรรมาภิบาลข้อมูล (NSDC-DG-108) ประกอบผนวก ข

๖.๓.๓ ให้ส่วนงานบริหารจัดการข้อมูล จัดทำแผนเตรียมความพร้อมกรณีเกิดเหตุฉุกเฉิน หรือแผนเผชิญเหตุเป็นรายกรณี (เช่นแผนเผชิญเหตุกรณีเกิดเหตุการณ์ข้อมูลรั่วไหล) เพื่อให้สามารถสกัดยับยั้งกู้คืนข้อมูลหรือปรับแก้ไขปัญหา ฟื้นฟูสภาพแวดล้อมที่เกี่ยวข้องกับข้อมูล เพื่อให้สามารถนำข้อมูลกลับมาใช้งานได้ตามปกติโดยเร็ว อย่างมีคุณภาพ และไม่ส่งผลกระทบต่อภารกิจ ภาพลักษณ์ และความเชื่อมั่นของหน่วยงานของรัฐ ภาคเอกชน และสังคมทั่วไป ทั้งนี้แผนเตรียมความพร้อมกรณีเกิดเหตุฉุกเฉิน หรือแผนเผชิญเหตุต้องกำหนดรายละเอียด ตามอนุผนวก ๙ แผนเผชิญเหตุกรณีเกิดเหตุฉุกเฉิน (NSDC-DG-109) ประกอบผนวก ข อย่างน้อย ดังนี้

๖.๓.๓.๑ กระบวนการปฏิบัติในการเผชิญเหตุการณ์

๖.๓.๓.๒ ผู้รับผิดชอบตามกระบวนการปฏิบัติในการเผชิญเหตุ

๖.๓.๓.๓ การรายงานเหตุและกรอบระยะเวลาในการรายงาน เพื่อให้หัวหน้าส่วนงานบริหารจัดการข้อมูลทราบ โดยมีรายละเอียดการรายงาน ดังนี้

๖.๓.๓.๓ (๑) คำอธิบายลักษณะเหตุการณ์

๖.๓.๓.๓ (๒) ผลที่อาจเกิดขึ้นจากเหตุการณ์ ความเสี่ยงต่อเจ้าของข้อมูล

๖.๓.๓.๓ (๓) มาตรการที่เสนอแนะหรือแนวทางบรรเทาเหตุ หรือผลกระทบที่อาจเกิดขึ้น

๖.๓.๓.๓ (๔) ผู้ประสานหรือเจ้าหน้าที่ติดต่อเพื่อสอบถามข้อมูลเหตุการณ์

๖.๓.๓.๔ กำหนดแนวทางการเปลี่ยนแปลงการปฏิบัติด้านข้อมูลที่เกี่ยวข้องในระหว่างการดำเนินการเผชิญเหตุ

๖.๓.๓.๕ สรุปรายงานเหตุการณ์ และนำสาเหตุการเกิดเหตุการณ์มาวิเคราะห์เพื่อหาแนวทางในการป้องกันการเกิดเหตุ

๖.๓.๔ เมื่อเกิดเหตุฉุกเฉินที่มีความเสี่ยงต่อข้อมูล ให้ดำเนินการดังนี้

๖.๓.๔.๑ ให้ผู้ตรวจพบแจ้งให้ผู้รับผิดชอบตามกระบวนการปฏิบัติในการเผชิญเหตุ หรือผู้ประสานหรือเจ้าหน้าที่ติดต่อเพื่อสอบถามข้อมูลเหตุการณ์ ทราบ เพื่อดำเนินการตามกระบวนการปฏิบัติในการเผชิญเหตุการณ์นั้น ๆ ตามข้อ ๖.๓.๓.๑

๖.๓.๔.๒ ให้ผู้รับผิดชอบตามกระบวนการปฏิบัติในการเผชิญเหตุ ประเมินความเสี่ยงและผลกระทบในทันที โดยใช้แบบฟอร์ม ตามอนุผนวก ๒๑ การประเมินความเสี่ยงภัยและผลกระทบ (NSDC-DG-221) ประกอบผนวก ค

๖.๓.๔.๓ ให้ผู้ประสานหรือเจ้าหน้าที่ติดต่อเพื่อสอบถามข้อมูลเหตุการณ์ แจ้งรายละเอียดและผลกระทบแก่ผู้ใช้งานข้อมูล และผู้มีส่วนได้ส่วนเสีย จนกว่าสถานการณ์จะคลี่คลายหรือกลับมาเป็นปกติ ทั้งนี้ให้รวบรวมรายละเอียดเกี่ยวกับเหตุการณ์ หรือหลักฐานทางดิจิทัลต่าง ๆ เพื่อใช้ประกอบการกำหนดมาตรการป้องกันการเกิดเหตุการณ์ซ้ำ

๖.๔ แนวปฏิบัติด้านการวัดและประเมินผลการขับเคลื่อนการบูรณาการ

วัตถุประสงค์หลักของวัดและประเมินผลการขับเคลื่อนการดำเนินการ เพื่อให้มีระบบประเมินความพร้อมในการธรรมาภิบาลข้อมูล รวมทั้งมีการตรวจสอบรายละเอียด ทิศทางการปฏิบัติให้เป็นไปตามเป้าหมายและตัวชี้วัดที่ส่วนงานบริหารจัดการข้อมูลได้กำหนดไว้ ทั้งในมิติด้านนโยบาย มาตรฐาน การดำเนินการ ผลสัมฤทธิ์ และผลกระทบจากการดำเนินการธรรมาภิบาลข้อมูลระดับบูรณาการ เพื่อให้มีหลักฐานเชิงประจักษ์อันนำไปสู่การปรับปรุงแก้ไข ยกระดับธรรมาภิบาลข้อมูล ให้มีมาตรฐาน เป็นสากล เชื่อถือได้ อย่างเป็นรูปธรรม ดังนั้นจึงกำหนดขอบเขตงานดังต่อไปนี้

๖.๔.๑ ผู้ที่มีส่วนได้ส่วนเสียในกระบวนการ มีจำนวน ๑๓ กลุ่ม ประกอบด้วย : (๑) ผู้บริหารข้อมูลระดับสูง (๒) คณะกรรมการประเมินความพร้อมและการดำเนินการธรรมาภิบาลข้อมูล (๓) ทีมบริกรข้อมูล กอ.รมน. (๔) เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (๕) ส่วนงานบริหารจัดการข้อมูล (๖) ทีมบริหารจัดการข้อมูล (๗) ส่วนงานเจ้าของข้อมูล (๘) หน่วยงานเจ้าของข้อมูล (๙) ผู้ประสานหรือเจ้าหน้าที่ติดต่อเพื่อสอบถามข้อมูลเหตุการณ์ (๑๐) ผู้สร้างข้อมูล (๑๑) ผู้ใช้งานข้อมูล (๑๒) เจ้าของข้อมูลส่วนบุคคล และ (๑๓) ผู้มีส่วนได้ส่วนเสียอื่น ๆ

๖.๔.๒ ให้ ผู้บริหารข้อมูลระดับสูง กอ.รมน. แต่งตั้งคณะกรรมการประเมินความพร้อมและการดำเนินการธรรมาภิบาลข้อมูล กอ.รมน. มีหน้าที่ตรวจสอบ วัดผล และประเมินความพร้อมและการดำเนินการเกี่ยวกับการธรรมาภิบาลข้อมูล ภายใต้กรอบเป้าหมาย และตัวชี้วัดด้านนโยบาย มาตรฐาน และแนวปฏิบัติที่อยู่ในกรอบความรับผิดชอบทั้งปวงของ กอ.รมน. โดยมีองค์ประกอบ ดังนี้

๖.๔.๒.๑ ประธานกรรมการ เป็นนายทหารสัญญาบัตรระดับชั้นยศ พล.ต. หรือข้าราชการพลเรือนระดับ ๙ หรือเทียบเท่าขึ้นไป

๖.๔.๒.๒ กรรมการ และเลขานุการ เป็นนายทหารระดับสัญญาบัตร หรือข้าราชการพลเรือนระดับ ๘ หรือเทียบเท่าขึ้นไป จำนวนไม่น้อยกว่า ๔ คน

๖.๔.๒.๓ ทั้งนี้ องค์ประกอบในคณะกรรมการฯ ต้องไม่ใช่บุคลากรของทีมบริกรข้อมูล กอ.รมน.

๖.๔.๓ ให้คณะกรรมการประเมินความพร้อมและการดำเนินการธรรมาภิบาลข้อมูล จัดทำแผนและดำเนินการ เพื่อตรวจสอบ วัดผล และประเมินความพร้อม รวมถึงผลการปฏิบัติในทุกขั้นตอนการธรรมาภิบาลของวงจรชีวิตข้อมูล ในข้อ ๖.๒ – ๖.๓ ทั้งนี้ให้ความสำคัญในเรื่อง การรักษาความมั่นคงปลอดภัย การคุ้มครองข้อมูลส่วนบุคคล การป้องกันการรั่วไหล คุณภาพข้อมูล และการเก็บประวัติหลักฐาน เป็นสำคัญ โดยสรุปรายงานผลการปฏิบัติประจำปีงบประมาณ ให้หัวหน้าส่วนงานบริหารจัดการข้อมูลทราบ ตามอนุผนวก ๑๐ รายงานการปฏิบัติด้านการธรรมาภิบาลข้อมูล (NSDC-DG-110) ประกอบผนวก ข

๖.๔.๔ ให้ผู้ที่มีความเกี่ยวข้องในส่วนงาน รับทราบผลการตรวจสอบ วัดผล และประเมินความพร้อมหรือผลการปฏิบัติ และร่วมมือกับคณะกรรมการประเมินความพร้อมและการดำเนินการธรรมาภิบาลข้อมูล เพื่อจัดทำแผนดำเนินการเพื่อแก้ไขและป้องกัน (Corrective and Preventive Action Plan : CPAP) รวมทั้งปรับเป้าหมายและตัวชี้วัดการธรรมาภิบาลข้อมูลของส่วนงาน ที่สะท้อนข้อเท็จจริงจากผลการตรวจสอบ วัดผลและประเมิน และสอดคล้องกับแนวทางนโยบายที่คณะกรรมการธรรมาภิบาลข้อมูลได้ให้ความเห็นชอบเพื่อยกระดับการธรรมาภิบาลข้อมูลของ กอ.รมน. ในห้วงระยะต่อไป ก่อนเสนอให้หัวหน้าส่วนงานบริหารจัดการข้อมูล พิจารณาดำเนินการ ตามอนุผนวก ๒๒ แบบฟอร์มการแก้ไขและป้องกัน (NSDC-DG-222) ประกอบผนวก ค

บทที่ ๖ เป็นบทที่มีเนื้อหาสำคัญ เนื่องจากเป็นการกำหนดขอบเขตงาน ขั้นตอนการปฏิบัติของผู้ที่มีส่วนได้ส่วนเสีย กับการธรรมาภิบาลข้อมูลระดับบูรณาการ ซึ่งเป็นการรวบรวมข้อมูลที่เกี่ยวกับงานด้านความมั่นคงของประเทศ จากหน่วยงานของรัฐและภาคเอกชน โดยมีประเด็นหลักครอบคลุมการกำหนดทิศทาง เป้าหมายและการปฏิบัติ ทั้งในด้านการขับเคลื่อนงานยามปกติ การบริหารจัดการความเสี่ยงในสถานการณ์ฉุกเฉิน และการวัดและประเมินผลที่นำไปสู่การปรับปรุงพัฒนาอย่างเป็นวงรอบต่อเนื่อง อย่างไรก็ตามการที่จะขับเคลื่อนงานให้เกิดการบูรณาการข้อมูลด้านความมั่นคงแบบองค์รวม ซึ่งเป็นเป้าหมายสำคัญของแผนแม่บทภายใต้ยุทธศาสตร์ชาติประเด็นความมั่นคง ดังนั้น กอ.รมน. ในฐานะศูนย์กลางข้อมูลด้านความมั่นคงและผู้ประมวลผลข้อมูลส่วนบุคคล โดยมีส่วนงานบริหารจัดการข้อมูล เป็นหน่วยรับผิดชอบหลัก จำเป็นต้องประชาสัมพันธ์ อบรมหรือมีกิจกรรมเพื่อเสริมสร้างความตระหนักรู้ ความเข้าใจ และพัฒนาทักษะประสบการณ์ ให้กับผู้ที่มีส่วนได้ส่วนเสียในทุกขั้นตอนการปฏิบัติของวงจรชีวิตข้อมูลระดับบูรณาการ เพื่อให้เกิดความเชื่อมั่น ได้รับความเชื่อถือและเป็นที่ยอมรับจากทุกหน่วยงานและบุคลากรที่เกี่ยวข้อง ทั้งในด้านความชัดเจนในขั้นตอนปฏิบัติ การรักษาความปลอดภัยการรักษาชั้นความลับ การคุ้มครองข้อมูลส่วนบุคคล และความน่าเชื่อถือในคุณภาพข้อมูลที่ต้องมีความถูกต้อง ครบถ้วน สอดคล้องต้องกัน เป็นปัจจุบัน ตรงตามความต้องการ และพร้อมใช้งาน อย่างเป็นระบบต่อไป

ภาคผนวก

ผนวก ก บรรณานุกรม

๑. ศรีสมรัก อินทุจันทร์ยง. (๒๕๕๖). Business Intelligence กับการบริหาร วางแผน และตัดสินใจ. *วารสารบริหารธุรกิจ คณะพาณิชยศาสตร์และการบัญชี มหาวิทยาลัยธรรมศาสตร์*, ๓๖(๑๓๗), ๓-๗.

๒. สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์. (๒๕๖๔). *ปัญญาประดิษฐ์ในการให้บริการของภาครัฐ*. เข้าถึงได้จาก https://www.etda.or.th/th/Useful-Resource/Knowledge-Sharing/Articles/AI-in-Government-Services.aspx

๓. พระราชบัญญัติการพัฒนาดิจิทัลเพื่อเศรษฐกิจและสังคม พ.ศ. ๒๕๖๐. (๒๕๖๐, ๒๔ มกราคม). *ราชกิจจานุเบกษา*. เล่ม ๑๓๔ ตอนที่ ๑๐ ก, หน้า ๑–๒๓.

๔. ประกาศคณะกรรมการพัฒนารัฐบาลดิจิทัล เรื่อง แผนพัฒนารัฐบาลดิจิทัลของประเทศไทย พ.ศ. ๒๕๖๓ – ๒๕๖๕ (๒๕๖๔, ๑๔ มิถุนายน). *ราชกิจจานุเบกษา.* เล่ม ๑๓๘ ตอนพิเศษ ๑๒๗ ง, หน้า ๓๒.

๕. Hupperz, M., Gür, I., Möller, F., & Otto, B. (2021). *What is a Data-Driven Organization?*. Twenty-Seventh Americas Conference on Information Systems, Montreal.

๖. รัฐธรรมนูญแห่งราชอาณาจักรไทย. (๒๕๖๐, ๖ เมษายน). *ราชกิจจานุเบกษา*. เล่ม ๑๓๔ ตอนที่ ๔๐ ก, หน้า ๑–๙๐.

๗. พระราชบัญญัติการรักษาความมั่นคงภายในราชอาณาจักร พ.ศ. ๒๕๕๑. (๒๕๕๑, ๒๗ กุมภาพันธ์). *ราชกิจจานุเบกษา*. เล่ม ๑๒๕ ตอนที่ ๓๙ ก, หน้า ๓๓–๔๔.

๘. พิจารณาอนุมัติแผนปฏิบัติการด้านการบูรณาการข้อมูลด้านความมั่นคง ระยะที่ ๑ (พ.ศ. ๒๕๖๓ - ๒๕๖๕) (๒๕๖๒, ๑๓ ธันวาคม). *สำนักงานสภาความมั่นคงแห่งชาติ*. ที่ นร ๐๘๐๑.๑๓/๑๐๐๗๙

๙. พระราชบัญญัติการบริหารงานและการให้บริการภาครัฐผ่านระบบดิจิทัล พ.ศ. ๒๕๖๒. (๒๕๖๒, ๒๒ พฤษภาคม). *ราชกิจจานุเบกษา*. เล่ม ๑๓๖ ตอนที่ ๖๗ ก, หน้า ๕๗–๖๖.

๑๐. ประกาศคณะกรรมการพัฒนารัฐบาลดิจิทัล เรื่อง ธรรมาภิบาลข้อมูลภาครัฐ. (๒๕๖๓, ๓๑ มีนาคม). *ราชกิจจานุเบกษา*. เล่ม ๑๓๗ ตอนพิเศษ ๗๔ ง, หน้า ๔๗–๔๘.

๑๑. พระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ.๒๕๔๐. (๒๕๔๐, ๑๐ กันยายน). *ราชกิจจานุเบกษา*. เล่ม ๑๑๔ ตอนที่ ๔๖ ก, หน้า ๑–๑๖.

๑๒. พระราชบัญญัติข่าวกรองแห่งชาติ พ.ศ. ๒๕๖๒. (๒๕๖๒, ๑๖ เมษายน). *ราชกิจจานุเบกษา*. เล่ม ๑๓๖ ตอนที่ ๕๐ ก, หน้า ๒๒–๒๘.

๑๓. ระเบียบว่าด้วยการรักษาความลับของทางราชการ พ.ศ. ๒๕๔๔. (๒๕๔๔, ๒๓ กุมภาพันธ์). *ราชกิจจานุเบกษา*. เล่ม ๑๑๘ ตอนพิเศษ ๑๘ ง, หน้า ๒๘–๔๗.

๑๔. ระเบียบว่าด้วยการรักษาความลับของทางราชการ (ฉบับที่ ๒) พ.ศ. ๒๕๖๑. (๒๕๖๑, ๒๖ มิถุนายน). *ราชกิจจานุเบกษา.* เล่ม ๑๓๕ ตอนพิเศษ ๑๔๘ ง, หน้า ๑–๓.

๑๕. ระเบียบสำนักนายกรัฐมนตรีว่าด้วยการรักษาความปลอดภัยแห่งชาติ พ.ศ. ๒๕๕๒. (๒๕๕๒, ๑๓ มีนาคม). *ราชกิจจานุเบกษา*. เล่ม ๑๒๖ ตอนพิเศษ ๓๙ ง, หน้า ๔–๒๒.

๑๖. ระเบียบสำนักนายกรัฐมนตรีว่าด้วยการรักษาความปลอดภัยแห่งชาติ (ฉบับที่ ๓) พ.ศ. ๒๕๖๐. (๒๕๖๐, ๒๒ พฤศจิกายน). *ราชกิจจานุเบกษา*. เล่ม ๑๓๔ ตอนพิเศษ ๒๘๕ ง, หน้า ๑–๖.

๑๗. พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒. (๒๕๖๒, ๒๗ พฤษภาคม). *ราชกิจจานุเบกษา*. เล่ม ๑๓๖ ตอนที่ ๖๙ ก, หน้า ๒๐–๕๑.

๑๘. พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒. (๒๕๖๒, ๒๗ พฤษภาคม). *ราชกิจจานุเบกษา*. เล่ม ๑๓๖ ตอนที่ ๖๙ ก, หน้า ๕๒–๙๕.

๑๙. Handerson, D., Earley, S., Brackett, M. & Mosley M. (2009). *The DAMA Guide to The Data Management Body of Knowledge*. First Edition. United States of America. Technics Publications, LLC.

๒๐. ณัฏฐ์ณพัชร์ อ่อนตาม. (๒๕๖๒). เทคนิคการบริหารงานแบบ PDCA (Deming Cycle). *วารสารสมาคมพัฒนาวิชาชีพการบริหารการศึกษาแห่งประเทศไทย*, ๑(๓), ๓๙-๔๖.

๒๑. ขออนุมัติแผนปฏิบัติราชการประจำปีงบประมาณ พ.ศ. ๒๕๖๕ ของ กอ.รมน. (๒๕๖๕, ๗ กุมภาพันธ์). *สำนักนโยบายและยุทธศาสตร์ความมั่นคง กองอำนวยการรักษาความมั่นคงภายในราชอาณาจักร*. ที่ นร ๕๑๐๓/๑๘๑

ผนวก ข บัญชีรายการ ระเบียบ มาตรฐาน และข้อปฏิบัติ

อนุผนวก ๑ การสร้าง จัดเก็บ และจัดเก็บถาวร (ISOC-DG-101)
การสร้าง จัดเก็บ และจัดเก็บถาวร (NSDC-DG-101)

อนุผนวก ๒ การรักษาความปลอดภัยเกี่ยวกับข้อมูล (ISOC-DG-102)
การรักษาความปลอดภัยเกี่ยวกับข้อมูล (NSDC-DG-102)

อนุผนวก ๓ การคุ้มครองข้อมูลส่วนบุคคล (ISOC-DG-103)
การคุ้มครองข้อมูลส่วนบุคคล (NSDC-DG-103)

อนุผนวก ๔ การควบคุมคุณภาพข้อมูล (ISOC-DG-104)
การควบคุมคุณภาพข้อมูล (NSDC-DG-104)

อนุผนวก ๕ ข้อตกลงร่วมเกี่ยวกับการเผยแพร่ข้อมูล (ISOC-DG-105)
ข้อตกลงร่วมเกี่ยวกับการเผยแพร่ข้อมูล (NSDC-DG-105)

อนุผนวก ๖ มาตรการการเผยแพร่ข้อมูลออกสู่สาธารณะ (ISOC-DG-106)
มาตรการการเผยแพร่ข้อมูลออกสู่สาธารณะ (NSDC-DG-106)

อนุผนวก ๗ การเข้ารหัสข้อมูล (ISOC-DG-107)
การเข้ารหัสข้อมูล (NSDC-DG-107)

อนุนนวก ๘ การประเมินความพร้อมการธรรมาภิบาลข้อมูล (ISOC-DG-108)
การประเมินความพร้อมการธรรมาภิบาลข้อมูล (NSDC-DG-108)

อนุผนวก ๙ แผนเผชิญเหตุกรณีเกิดเหตุฉุกเฉิน (ISOC-DG-109)
แผนเผชิญเหตุกรณีเกิดเหตุฉุกเฉิน (NSDC-DG-109)

อนุผนวก ๑๐ รายงานการปฏิบัติด้านการธรรมาภิบาลข้อมูล (ISOC-DG-110)
รายงานการปฏิบัติด้านการธรรมาภิบาลข้อมูล (NSDC-DG-110)

ผนวก ค บัญชีรายการ แบบฟอร์มที่ใช้สำหรับการบันทึก

อนุผนวก ๑ การประเมินความเสี่ยงของข้อมูล (ISOC-DG-201)
การประเมินความเสี่ยงของข้อมูล (NSDC-DG-201)

อนุผนวก ๒ แบบฟอร์มเมทาดาตา (ISOC-DG-202)
แบบฟอร์มเมทาดาตา (NSDC-DG-202)

อนุผนวก ๓ การตรวจสอบการปฏิบัติด้านข้อมูล (ISOC-DG-203)
การตรวจสอบการปฏิบัติด้านข้อมูล (NSDC-DG-203)

อนุผนวก ๔ การตรวจสอบการรักษาความมั่นคงปลอดภัย (ISOC-DG-204)
การตรวจสอบการรักษาความมั่นคงปลอดภัย (NSDC-DG-204)

อนุผนวก ๕ การตรวจสอบการคุ้มครองข้อมูลส่วนบุคคล (ISOC-DG-205)
การตรวจสอบการคุ้มครองข้อมูลส่วนบุคคล (NSDC-DG-205)

อนุผนวก ๖ การตรวจสอบการรักษาความปลอดภัยของระบบและเครือข่าย (ISOC-DG-206)
การตรวจสอบการรักษาความปลอดภัยของระบบและเครือข่าย (NSDC-DG-206)

อนุผนวก ๗ การบันทึกประวัติการสำรองหรือกู้คืนข้อมูล (ISOC-DG-207)
การบันทึกประวัติการสำรองหรือกู้คืนข้อมูล (NSDC-DG-207)

อนุผนวก ๘ บัญชีคุมข้อมูลปกติ (ISOC-DG-208)
บัญชีคุมข้อมูลปกติ (NSDC-DG-208)

อนุผนวก ๙ บัญชีคุมข้อมูลพิเศษ (ISOC-DG-209)
บัญชีคุมข้อมูลพิเศษ (NSDC-DG-209)

อนุผนวก ๑๐ การขอความยินยอมให้ข้อมูล (ISOC-DG-210)
การขอความยินยอมให้ข้อมูล (NSDC-DG-210)

อนุผนวก ๑๑ การบันทึกประวัติการเข้าใช้งานข้อมูล (ISOC-DG-211)
การบันทึกประวัติการเข้าใช้งานข้อมูล (NSDC-DG-211)

อนุผนวก ๑๒ การบันทึกการตรวจสอบประวัติการเข้าใช้งานข้อมูล (ISOC-DG-212)
การบันทึกการตรวจสอบประวัติการเข้าใช้งานข้อมูล (NSDC-DG-212)

อนุผนวก ๑๓ การบันทึกการระงับการเข้าถึงข้อมูล (ISOC-DG-213)
การบันทึกการระงับการเข้าถึงข้อมูล (NSDC-DG-213)

อนุผนวก ๑๔ รายการบัญชีข้อมูลเผยแพร่ (ISOC-DG-214)
รายการบัญชีข้อมูลเผยแพร่ (NSDC-DG-214)

อนุผนวก ๑๕ การบันทึกประวัติการเผยแพร่ข้อมูล (ISOC-DG-215)
การบันทึกประวัติการเผยแพร่ข้อมูล (NSDC-DG-215)

อนุผนวก ๑๖ บัญชีคุมข้อมูลถาวร (ISOC-DG-216)
บัญชีคุมข้อมูลถาวร (NSDC-DG-216)

อนุผนวก ๑๗ บัญชีขอทำลายข้อมูล (ISOC-DG-217)
บัญชีขอทำลายข้อมูล (NSDC-DG-217)

อนุผนวก ๑๘ บัญชีการทวนสอบขอทำลายข้อมูล (ISOC-DG-218)
บัญชีการทวนสอบขอทำลายข้อมูล (NSDC-DG-218)

อนุผนวก ๑๙ บัญชีคุมข้อมูลทำลาย (ISOC-DG-219)
บัญชีคุมข้อมูลทำลาย (NSDC-DG-219)

อนุผนวก ๒๐ การประเมินความเสี่ยง (ISOC-DG-220)
การประเมินความเสี่ยง (NSDC-DG-220)

อนุผนวก ๒๑ การประเมินความเสี่ยงภัยและผลกระทบ (ISOC-DG-221)
การประเมินความเสี่ยงภัยและผลกระทบ (NSDC-DG-221)

อนุผนวก ๒๒ แบบฟอร์มการแก้ไขและป้องกัน (ISOC-DG-222)
แบบฟอร์มการแก้ไขและป้องกัน (NSDC-DG-222)

ผนวก ง บัญชีรายการ ตัวอย่างเอกสารหรือคำแนะนำประกอบการจัดทำเอกสาร

อนุผนวก ๑ การจัดทำแบบจำลองสำหรับการออกแบบข้อมูล (ISOC-DG-301)
การจัดทำแบบจำลองสำหรับการออกแบบข้อมูล (NSDC-DG-301)

อนุผนวก ๒ การจัดทำมาตรฐานข้อมูล (ISOC-DG-302)
การจัดทำมาตรฐานข้อมูล (NSDC-DG-302)

อนุผนวก ๓ การจัดทำสถาปัตยกรรมข้อมูล (ISOC-DG-303)
การจัดทำสถาปัตยกรรมข้อมูล (NSDC-DG-303)

อนุผนวก ๔ การจัดทำเอกสารควบคุมการเข้าถึงข้อมูล (ISOC-DG-304)
การจัดทำเอกสารควบคุมการเข้าถึงข้อมูล (NSDC-DG-304)

บันทึกข้อความ

ส่วนราชการ สนย.กอ.รมน. (ส่วนปฏิบัติการข่าวสาร โทร. ๐ ๒๒๔๑ ๔๘๓๘, ๘๓๔๓๑)

ที่ นร ๕๑๐๓/๘๕๒ **วันที่** ๑๖ มิ.ย. ๖๕

เรื่อง ขออนุมัติธรรมาภิบาลข้อมูลด้านความมั่นคง กอ.รมน. พ.ศ. ๒๕๖๕

เรียน รอง ผอ.รมน./ผู้บริหารระดับสูงสุด กอ.รมน.

- เห็นควรอนุมัติตามที่ สนย.กอ.รมน. เสนอในข้อ ๔ พร้อมทั้งลงนามใน คำนำ ประกอบธรรมาภิบาลข้อมูลฯ ตามสิ่งที่ส่งมาด้วย ๔

พล.ท.
รองเลขาธิการ กอ.รมน.(๑)
มิ.ย. ๖๕

อนุมัติตามเสนอในหนังสือ ๔

พล.อ.
รอง ผอ.รมน./ผู้บริหารระดับสูงสุด
กอ.รมน.
๑๗ มิ.ย. ๖๕

พล.อ.
เลขาธิการ กอ.รมน.
๑๗ มิ.ย. ๖๕

บันทึกข้อความ

ส่วนราชการ สนย.กอ.รมน. (ส่วนปฏิบัติการข่าวสาร โทร. ๐ ๒๒๔๑ ๔๘๓๘, ๘๓๔๓๑)

ที่ นร ๕๑๐๓ / [illegible] **วันที่** ๒๖ มิ.ย. ๖๕

เรื่อง ขออนุมัติธรรมาภิบาลข้อมูลด้านความมั่นคง กอ.รมน. พ.ศ. ๒๕๖๕

เรียน รอง ผอ.รมน./ผู้บริหารระดับสูงสุด กอ.รมน.

อ้างถึง ๑. พ.ร.บ. การบริหารงานและการให้บริการภาครัฐผ่านระบบดิจิทัล พ.ศ. ๒๕๖๒
๒. ประกาศคณะกรรมการพัฒนารัฐบาลดิจิทัล เรื่อง ธรรมาภิบาลข้อมูลภาครัฐ ลง ๑๒ มี.ค. ๖๓
๓. คำสั่ง กอ.รมน. ที่ ๓๓๑/๒๕๖๕ ลง ๒๖ เม.ย. ๖๕
๔. หนังสือ สมช. ที่ นร ๑๘๐๑.๑๓/๑๐๐๗๙ ลง ๑๓ ธ.ค. ๖๒

สิ่งที่ส่งมาด้วย ๑. หนังสือ ศดม.กอ.รมน. ที่ นร ๕๑๒๐/๓๒๓ ลง ๙ มิ.ย. ๖๕
๒. (ร่าง) ธรรมาภิบาลข้อมูลด้านความมั่นคง กอ.รมน. พ.ศ. ๒๕๖๕ จำนวน ๑ ฉบับ
๓. เอกสารพิจารณาร่วมของ นขต.กอ.รมน. จำนวน ๑ ชุด
๔. คำนำ ประกอบธรรมาภิบาลข้อมูลด้านความมั่นคง กอ.รมน. พ.ศ. ๒๕๖๕ จำนวน ๑ ฉบับ

๑. ศดม.กอ.รมน. ขออนุมัติธรรมาภิบาลข้อมูลด้านความมั่นคง กอ.รมน. พ.ศ. ๒๕๖๕ รวมถึงวิสัยทัศน์ธรรมาภิบาลข้อมูลด้านความมั่นคง กอ.รมน. เพื่อให้บุคลากรและหน่วยงานที่เกี่ยวข้อง นำไปใช้และยึดถือปฏิบัติในการบริหารจัดการข้อมูลที่อยู่ในรูปแบบดิจิทัล ของ กอ.รมน. และของหน่วยงานภายนอกอื่น ๆ ที่ กอ.รมน. ได้บูรณาการเชื่อมโยงแลกเปลี่ยนเข้ามาใช้งานในฐานะศูนย์กลางข้อมูลด้านความมั่นคง รวมทั้งให้ข้อเสนอเพิ่มเติมในการเสริมสร้างองค์ความรู้ ความเข้าใจ เพื่อให้สามารถนำไปปฏิบัติได้อย่างต่อเนื่อง รายละเอียดตามสิ่งที่ส่งมาด้วย ๑ และ ๒ สรุปได้ดังนี้

๑.๑ วิสัยทัศน์และธรรมาภิบาลข้อมูลด้านความมั่นคง กอ.รมน. พ.ศ. ๒๕๖๕

๑.๑.๑ วิสัยทัศน์ธรรมาภิบาลข้อมูลของ กอ.รมน. : “กอ.รมน. เป็นองค์กรหลักในการบูรณาการข้อมูลเพื่อใช้สนับสนุนพันธกิจให้เกิดความมั่นคงของรัฐและความสงบสุขของประชาชน โดยมีระบบบริหารจัดการข้อมูลที่ดี มีคุณภาพ ปลอดภัย โปร่งใส และตรวจสอบได้”

๑.๑.๒ ธรรมาภิบาลข้อมูลด้านความมั่นคง กอ.รมน. พ.ศ. ๒๕๖๕

๑.๑.๒.๑ วัตถุประสงค์ในการจัดทำ

๑.๑.๒.๑ (๑) เพื่อให้มีกรอบนโยบายและแนวปฏิบัติในการบริหารจัดการและกำกับดูแลข้อมูลด้านความมั่นคงทั้งระบบที่เป็นมาตรฐานสากล สอดคล้องกับหลักธรรมาภิบาลข้อมูลภาครัฐ รวมถึง ระเบียบ กฎหมาย และนโยบายภาครัฐอื่น ๆ ที่เกี่ยวข้อง

๑.๑.๒.๑ (๒) เพื่อส่งเสริมการปรับปรุงพัฒนาระบบฐานข้อมูลของ กอ.รมน. รวมทั้งหน่วยงานของรัฐและภาคเอกชนที่เกี่ยวข้อง ให้มีมาตรฐานและเกื้อกูลต่อการเชื่อมโยงแลกเปลี่ยนข้อมูลกับศูนย์กลางข้อมูลด้านความมั่นคง

๑.๑.๒.๑ (๓) เพื่อสร้างความเชื่อมั่นและอำนวยความสะดวกให้กับ นขต.กอ.รมน. รวมทั้งหน่วยงานของรัฐและภาคเอกชน ที่สนับสนุนข้อมูลและการเชื่อมโยงแลกเปลี่ยนข้อมูล รวมทั้งการใช้ประโยชน์จากระบบบูรณาการข้อมูลเชิงวิเคราะห์ของศูนย์กลางข้อมูลด้านความมั่นคง

๑.๑.๒.๒ การกำหนดนโยบายธรรมาภิบาลข้อมูล แบ่งเป็น ๓ ด้าน ประกอบด้วย นโยบายขับเคลื่อนธรรมาภิบาลข้อมูลของส่วนงานใน กอ.รมน. นโยบายบูรณาการข้อมูลระหว่างหน่วยงาน และนโยบายการบริหารจัดการความเสี่ยง

/๑.๑.๒.๓ การกำหนด ...

๑.๑.๒.๓ การกำหนดโครงสร้างบุคลากรที่เกี่ยวข้องกับธรรมาภิบาลข้อมูล แบ่งเป็น ๓ กลุ่ม

๑.๑.๒.๓ (๑) โครงสร้างและความรับผิดชอบของบุคลากรระดับบริหาร ประกอบด้วย ผู้บริหารระดับสูงสุด กอ.รมน. ผู้บริหารเทคโนโลยีสารสนเทศระดับสูงของ กอ.รมน. ผู้บริหารข้อมูลระดับสูงของ กอ.รมน. ผู้บริหารด้านการรักษาความปลอดภัยระดับสูงของ กอ.รมน. คณะกรรมการธรรมาภิบาลข้อมูล กอ.รมน. ทีมบริกรข้อมูล กอ.รมน. ผู้เชี่ยวชาญเฉพาะทาง และเจ้าหน้าที่คุ้มครองข้อมูล

๑.๑.๒.๓ (๒) โครงสร้างและความรับผิดชอบของบุคลากรระดับปฏิบัติ ประกอบด้วย ส่วนงานเจ้าของข้อมูล (นขต.กอ.รมน.) ส่วนงานบริหารจัดการข้อมูล (ศดม.กอ.รมน.) ผู้ควบคุมข้อมูล ผู้ควบคุมข้อมูลส่วนบุคคล วิศวกรระบบ วิศวกรข้อมูล นักวิเคราะห์ข้อมูล และวิศวกรความมั่นคงปลอดภัยไซเบอร์

๑.๑.๒.๓ (๓) ความรับผิดชอบของผู้ที่มีส่วนได้ส่วนเสียอื่น ๆ ประกอบด้วย หน่วยงานภายนอกที่เป็นเจ้าของข้อมูล ผู้สร้างข้อมูล ผู้ใช้งานข้อมูล และเจ้าของข้อมูลส่วนบุคคล

๑.๑.๒.๔ ขอบเขตงานธรรมาภิบาลข้อมูล แบ่งเป็น ๔ กลุ่มงาน ประกอบด้วย ๑) แนวปฏิบัติและมาตรฐานข้อมูลในกรอบหน้าที่และอำนาจของ กอ.รมน. ๒) แนวปฏิบัติและมาตรฐานข้อมูลในกรอบความรับผิดชอบของศูนย์กลางข้อมูลด้านความมั่นคง ๓) แนวปฏิบัติเกี่ยวกับการบริหารจัดการความเสี่ยง และ ๔) แนวปฏิบัติเกี่ยวกับการวัดและประเมินผล

๑.๑.๒.๕ ผอ.ศดมกอ.รมน. เป็นผู้รักษาการให้เป็นไปตามธรรมาภิบาลข้อมูลด้านความมั่นคง กอ.รมน. พ.ศ. ๒๕๖๕

๑.๒ ข้อเสนอเพิ่มเติมในการเสริมสร้างองค์ความรู้

เนื่องด้วยธรรมาภิบาลข้อมูลด้านความมั่นคง กอ.รมน. พ.ศ. ๒๕๖๕ เป็นเรื่องใหม่ที่มีรายละเอียดเนื้อหาเกี่ยวข้องกับบุคลากรและส่วนงานใน กอ.รมน. รวมทั้งหน่วยงานภายนอกจำนวนมาก จึงเห็นสมควรจัดให้มีการฝึกอบรมเพื่อเสริมสร้างองค์ความรู้ ความเข้าใจให้สามารถนำไปใช้ปฏิบัติได้จริงอย่างต่อเนื่อง

๒. สนย.กอ.รมน. ขอเรียนชี้แจงดังนี้

๒.๑ ภายใต้ พ.ร.บ. การบริหารงานและการให้บริการภาครัฐผ่านระบบดิจิทัล พ.ศ. ๒๕๖๒ คณะกรรมการพัฒนารัฐบาลดิจิทัล ได้จัดทำและประกาศธรรมาภิบาลข้อมูลภาครัฐ เพื่อให้หน่วยงานของรัฐนำไปใช้เป็นกรอบในการจัดทำธรรมาภิบาลข้อมูลภาครัฐระดับหน่วยงาน รายละเอียดตามอ้างถึง ๑ และ ๒

๒.๒ คำสั่ง กอ.รมน. ที่ ๓๓๑/๒๕๖๕ ลง ๒๖ เม.ย. ๖๕ ได้มอบหมายภาระงานโดยแต่งตั้งให้ รอง ผอ.รมน. ปฏิบัติราชการแทน ผอ.รมน. ในฐานะผู้บริหารระดับสูงสุด (CEO) กอ.รมน. มีอำนาจและหน้าที่ในการกำหนดวิสัยทัศน์ ตัดสินใจ และอนุมัตินโยบายข้อมูล มาตรฐานข้อมูล แนวทางปฏิบัติงาน เกณฑ์วัดคุณภาพระเบียบ และข้อบังคับอื่น ๆ ที่เกี่ยวข้องกับข้อมูล รวมทั้งการจัดลำดับความสำคัญในการแก้ไขปัญหาที่เกี่ยวข้องกับข้อมูล รายละเอียดตามอ้างถึง ๓

๒.๓ นรม./ประธานสภาความมั่นคงแห่งชาติ ได้กรุณาลงนามอนุมัติและประกาศใช้แผนปฏิบัติการด้านการบูรณาการข้อมูลด้านความมั่นคง ระยะที่ ๑ (พ.ศ. ๒๕๖๓ - ๒๕๖๕) ซึ่งได้มอบหมายให้ กอ.รมน. เป็นหน่วยงานกลางทำหน้าที่เป็นศูนย์กลางข้อมูลด้านความมั่นคง และรับผิดชอบในการอำนวยการและประสานการปฏิบัติในการเชื่อมโยงแลกเปลี่ยนข้อมูลด้านความมั่นคงระหว่างหน่วยงานที่เกี่ยวข้อง รายละเอียดตามอ้างถึง ๔

/๒.๔ นขต.กอ.รมน. ...

๒.๔ นขต.กอ.รมน. ได้ตรวจสอบและร่วมพิจารณาให้ความเห็นชอบวิสัยทัศน์และ (ร่าง) ธรรมาภิบาลข้อมูลด้านความมั่นคง กอ.รมน. พ.ศ. ๒๕๖๕ แล้ว รายละเอียดตามสิ่งที่ส่งมาด้วย ๓

๓. สนย.กอ.รมน. พิจารณาแล้วเห็นว่า การขออนุมัติธรรมาภิบาลข้อมูลฯ ในข้อ ๑ เป็นการดำเนินการตามที่ได้กำหนดไว้ในประกาศคณะกรรมการพัฒนารัฐบาลดิจิทัล ตามข้อ ๒.๑ ซึ่งจะทำให้การดำเนินการตามแผนปฏิบัติการด้านการบูรณาการข้อมูลฯ ที่ได้อนุมัติไว้แล้ว ในการเป็นศูนย์กลางข้อมูลด้านความมั่นคง เป็นไปด้วยความเรียบร้อย โดย นขต.กอ.รมน. ได้ร่วมพิจารณาและให้ความเห็นชอบ (ร่าง) ธรรมาภิบาลข้อมูลฯ ดังกล่าวเรียบร้อยแล้ว ดังนั้น เพื่อให้การดำเนินการดังกล่าวเป็นไปด้วยความเรียบร้อย จึงเห็นสมควรอนุมัติธรรมาภิบาลข้อมูลด้านความมั่นคง กอ.รมน. พ.ศ. ๒๕๖๕ เพื่อยึดถือเป็นนโยบายและแนวทางปฏิบัติในการบริหารจัดการระบบข้อมูลในความรับผิดชอบของ กอ.รมน. ซึ่งมีทั้งข้อมูลของ กอ.รมน. และข้อมูลที่ กอ.รมน. บูรณาการการเชื่อมโยงจากแหล่งข้อมูลของหน่วยงานภาครัฐและภาคเอกชน ในฐานะเป็นศูนย์กลางข้อมูลด้านความมั่นคงของประเทศ รวมทั้งให้ ศดม.กอ.รมน. พิจารณาดำเนินการฝึกอบรมเพื่อเสริมสร้างองค์ความรู้ ความเข้าใจในเรื่องดังกล่าว ให้สามารถนำไปใช้ปฏิบัติได้จริงอย่างต่อเนื่อง ต่อไป

๔. ข้อเสนอ เห็นสมควรอนุมัติธรรมาภิบาลข้อมูลด้านความมั่นคง กอ.รมน. พ.ศ. ๒๕๖๕ ตามการพิจารณาในข้อ ๓

จึงเรียนมาเพื่อกรุณาอนุมัติตามเสนอในข้อ ๔ พร้อมทั้งลงนามใน คำนำ ประกอบธรรมาภิบาลข้อมูลฯ ตามสิ่งที่ส่งมาด้วย ๔ ทั้งนี้ อยู่ในอำนาจของ รอง ผอ.รมน./ผู้บริหารระดับสูงสุด กอ.รมน. ตามคำสั่ง กอ.รมน. ที่ ๓๓๑/๒๕๖๕ ลง ๒๖ เม.ย. ๖๕

พล.ท.
(ไพรุจน์ คำชุม)
ผอ.สนย.กอ.รมน.