หลักเกณฑ์การพัฒนาข้อมูลและสารสนเทศของกรมควบคุมมลพิษ
เรื่อง บททั่วไป คำนิยาม กฎเกณฑ์ที่เกี่ยวข้องและกระบวนการร่วมกับผู้มีส่วนได้ ส่วนเสีย

เพื่อประโยชน์ในการดำเนินงานและสร้างความเข้าใจที่ถูกต้องตรงกัน สำหรับการบริหารจัดการและดำเนินการจัดทำของการพัฒนาฐานข้อมูลและระบบสารสนเทศของกรมควบคุมมลพิษ ตลอดจนการควบคุมและตรวจสอบการดำเนินงานที่เกี่ยวข้องกับข้อมูล ตั้งแต่การสร้าง การจัดเก็บ การประมวลผล การใช้ การเผยแพร่ จนถึงการทำลาย คณะทำงานบริกรข้อมูล กรมควบคุมมลพิษ จึงกำหนดคำนิยามไว้ดังต่อไปนี้

<u>นิยามทั่วไป</u>

การกำกับดูแลข้อมูล (Data Governance) หมายถึง “การกำหนดสิทธิ หน้าที่และความรับผิดชอบของผู้มีส่วนได้ส่วนเสียในการบริหารจัดการข้อมูลทุกขั้นตอน เพื่อให้การได้มาและการนำไปใช้ข้อมูลของหน่วยงานภาครัฐถูกต้อง ครบถ้วน เป็นปัจจุบัน รักษาความเป็นส่วนบุคคล และสามารถเชื่อมโยงกันได้อย่างมีประสิทธิภาพและมั่นคงปลอดภัย โดยใช้ข้อมูลเป็นหลักในการขับเคลื่อนประเทศ เช่น การใช้ข้อมูลในการวิเคราะห์การตัดสินใจเชิงนโยบายและการบริหารราชการแผ่นดิน การเพิ่มประสิทธิภาพในการบริการประชาชน การเสริมสร้างและผลักดันธุรกิจที่เกิดจากการใช้นวัตกรรมข้อมูล”

ข้อมูล (Data) หมายถึง “ข้อเท็จจริงซึ่งใช้เป็นพื้นฐานสำหรับการอธิบายเหตุผล การสนทนา หรือการคำนวณ ซึ่งมีความสัมพันธ์กับกระบวนการปฏิบัติงาน เทคโนโลยีสารสนเทศ สถานที่ รวมถึงบุคลากร”

ฐานข้อมูล (Database) หมายถึง “กลุ่มข้อมูลที่มีความสัมพันธ์กันได้ถูกรวบรวมเข้าไว้ด้วยกัน ซึ่งสนับสนุนกิจกรรมของหน่วยงาน”

การรักษาความลับ (Confidentiality) หมายถึง “การรักษาข้อมูลตามสภาพของการจัดชั้นความลับ และมีการกำหนดสิทธิการเข้าถึงข้อมูลนั้น เนื่องจากข้อมูลในหน่วยงานอาจมีหลายประเภท ข้อมูลบางประเภทเป็นข้อมูลที่มีความสำคัญ หรืออ่อนไหว จึงต้องมีการรักษาความลับ เพื่อลดความเสี่ยงของการถูกคุกคามและเป็นการป้องกันการรั่วไหลของข้อมูลโดยมิชอบ”

ความถูกต้องของข้อมูล (Integrity) หมายถึง “การคงสภาพของข้อมูลหรือการรักษาความถูกต้องสมบูรณ์ของข้อมูลให้มีความถูกต้องและน่าเชื่อถือ รวมถึงมีการปกป้องข้อมูลให้ปราศจากการถูกเปลี่ยนแปลงโดยผู้ไม่มีสิทธิ”

ความพร้อมใช้งานของข้อมูล (Availability) หมายถึง “การพร้อมในการใช้งานอยู่เสมอ กล่าวคือ ข้อมูลต้องพร้อมสำหรับการใช้งานได้เสมอ รวมถึงมีการสำรองข้อมูลไว้เมื่อเกิดภัยพิบัติหรือเหตุการณ์ที่ไม่คาดฝัน”

ข้อมูลส่วนบุคคล (Personal Data) หมายถึง “ข้อมูลเกี่ยวกับสิ่งเฉพาะตัวของบุคคล ที่ทำให้สามารถระบุตัวหรือรู้ตัวของบุคคลนั้น ๆ ได้”

ข้อมูลความมั่นคง (Security Data) หมายถึง “ข้อมูลเกี่ยวกับความมั่นคงของรัฐที่ทำให้เกิดความสงบเรียบร้อย การมีเสถียรภาพความเป็นปึกแผ่น ปลอดภัยจากภัยคุกคาม เป็นต้น”

ข้อมูลความลับทางราชการ (Government Secret Data) หมายถึง “ข้อมูลที่อยู่ในความครอบครองหรือควบคุมดูแลของหน่วยงานของรัฐที่มีคำสั่งไม่ให้มีการเปิดเผย และมีการกำหนดชั้นความลับของข้อมูล”

ข้อมูลสาธารณะ (Public Data) หมายถึง “ข้อมูลที่สามารถเปิดเผยได้ สามารถนำไปใช้ได้อย่างอิสระ ไม่ว่าจะเป็นข้อมูลข่าวสาร ข้อมูลส่วนบุคคล ข้อมูลอิเล็กทรอนิกส์ เป็นต้น”

นิยามเฉพาะ

สถานีตรวจวัดอัตโนมัติ (Automatic Monitor Station) หมายถึง “สถานที่หรือเครื่องมืออุปกรณ์ของกรมควบคุมมลพิษ ซึ่งสามารถทำงานได้ด้วยตัวเองหรือทำงานร่วมกับอุปกรณ์อื่น เพื่อใช้ตรวจวัด เก็บ บันทึก รวบรวม ส่งต่อ ซึ่งข้อเท็จจริงของสภาพแวดล้อมหรือมลพิษ ทั้งทางน้ำ อากาศ เสียง ความสั่นสะเทือน หรือ ขยะกากของเสียและสารเคมี”

พารามิเตอร์ (Parameter) หมายถึง “ค่าคงที่หรือค่าคงตัวเฉพาะการณ์ที่กำหนดขึ้น ตามปัจจัยที่กำหนดหรือปัจจัยที่ต้องการ”

รูปแบบ ลักษณะของข้อมูล

เพื่อการใช้งานได้ตามวัตถุประสงค์ที่กำหนด คณะทำงานบริกรข้อมูล กรมควบคุมมลพิษ จึงกำหนดรูปแบบ ลักษณะ หรือรายละเอียดของข้อมูลประเภทต่าง ๆ อย่างน้อย ตามเอกสารที่แนบท้ายนี้

<u>รายละเอียดแนบท้าย</u>

ก) แบบฟอร์มการจัดทำเมทาดาตา ๒๒ หัวข้อ (Metadata Form) ตามที่กระทรวงทรัพยากรธรรมชาติและสิ่งแวดล้อมกำหนด

ข) Data dictionary / Data catalog

ค) Data workflow diagram

หลักเกณฑ์การพัฒนาข้อมูลและสารสนเทศของกรมควบคุมมลพิษ
เรื่อง แนวปฏิบัติในการออกแบบความคิดเชิงนวัตกรรมด้านข้อมูล (Data Innovation Guideline)

เพื่อประโยชน์ในการดำเนินงานและสร้างความเข้าใจที่ถูกต้องตรงกัน สำหรับการบริหารจัดการและดำเนินการจัดทำของการพัฒนาฐานข้อมูลและระบบสารสนเทศของกรมควบคุมมลพิษ ตลอดจนการควบคุมและตรวจสอบการดำเนินงานที่เกี่ยวข้องกับข้อมูล ตั้งแต่การกำหนดโจทย์ ประดิษฐ์ เชื่อมโยง ปฏิบัติการประมวลผล การใช้ การเผยแพร่ จนถึงการทำลาย คณะทำงานบริกรข้อมูล กรมควบคุมมลพิษ จึงกำหนดแนวปฏิบัติเกี่ยวกับนวัตกรรมไว้ดังต่อไปนี้

<u>นิยามเฉพาะ</u>

ความเป็นส่วนบุคคล ความปลอดภัย หรือความหมายอย่างเดียวกัน (Privacy / Compliance / Security) หมายถึง สำหรับกิจกรรม การกระทำ บางประเภท การใช้งานของข้อมูลนั้น ๆ จำเป็นต้องปฏิบัติตามกฎข้อบังคับในลักษณะใดลักษณะหนึ่งที่กำหนด ให้ผู้ใช้หรือผู้รับผิดชอบดำเนินการเช่นว่านั้นตามแนวปฏิบัติที่กำหนดไว้เสมอ ทั้งที่เป็นความจำเป็นทางกฎหมาย และที่เป็นความคาดหวังจากผู้ใช้บริการ

สถาปัตยกรรม โครงสร้าง หรือความหมายอย่างเดียวกัน (Architecture / Integration / Restructuring) หมายถึง การดำเนินการใด ซึ่งส่งผลให้มีการวางสถาปัตยกรรมทางด้านระบบข้อมูลใหม่ หรือจำเป็นต้องเชื่อมโยงและหรือบูรณาการกับหน่วยงานอื่น ทั้งภายในและภายนอกองค์กร

คลังข้อมูล ข้อมูลทางธุรกิจ หรือความหมายอย่างเดียวกัน (Data Warehouse & Business Intelligence) หมายถึง การพัฒนาคลังข้อมูลใหม่ หรือมีการนำเครื่องมือ BI เข้ามาใช้ในองค์กร

บุคคล กลุ่มบุคลากรและคณะทำงานเกี่ยวกับข้อมูล (People & Organization Bodies) ประกอบด้วยบุคคลหลายบทบาทหน้าที่ ดังนี้

- ผู้มีส่วนได้ส่วนเสียกับข้อมูล (Data Stakeholders) ให้หมายความรวมถึง บุคคล หรืออาจจะเป็นหน่วยงานหรือกลุ่มคนที่สร้างข้อมูล หรือใช้ข้อมูล

○ สำนักงานธรรมาภิบาลข้อมูล (Data Governance Office) ให้หมายความรวมถึง กลุ่มคนซึ่งทำกิจกรรมต่าง ๆ เพื่อสนับสนุนงานทั่วไปเกี่ยวกับ data governance (เช่น การเก็บรวบรวมผลลัพธ์คุณภาพข้อมูล การสื่อสารกับหน่วยงานอื่น ๆ ในองค์กร การจัดอบรมสัมนา หรือให้ความช่วยเหลือโดยทั่วไปเกี่ยวกับงานข้อมูล)

○ ผู้เชี่ยวชาญข้อมูล (Data Stewards) ให้หมายความรวมถึง บุคคลอื่น ซึ่งอาจแบ่งได้เป็นหลายระดับขึ้นอยู่กับความซับซ้อนของข้อมูลในองค์กร ตลอดจนผู้ทำงานและให้คำปรึกษาเกี่ยวกับนิยามหรือมาตรฐานข้อมูล หรือกำหนดนโยบายเกี่ยวกับข้อมูล และอาจรวมไปถึงกำหนดเกณฑ์คุณภาพข้อมูลด้วย

หมวด ๑
การใช้งานระบบสารสนเทศ (IT Work System)

๑. มีการจัดทำคู่มือการใช้งานระบบสารสนเทศ ระบบงาน หรือระบบฐานข้อมูล
๒. ผู้ใช้งานจำเป็นที่จะต้องใช้งานอยู่ภายใต้กรอบของการดำเนินงาน และคู่มือ
๓. ผู้ใช้งานจำเป็นที่จะต้องศึกษาคู่มืออย่างละเอียดถี่ถ้วน
๔. ผู้ใช้งานจะต้องไม่กระทำการอันใด อันเป็นการรบกวนระบบให้ทำงานผิดพลาด
๕. ผู้ใช้งานจะต้องไม่กระทำการอันใด เพื่อเข้าถึงสิทธิ์อันนอกเหนือจากที่ได้รับ
๖. หากพบข้อผิดพลาดใด ๆ จะต้องดำเนินการแจ้งผู้ดูแลระบบโดยทันที

หมวด ๒
การพัฒนาระบบสารสนเทศ (IT System Development)

๑. ระบบสารสนเทศที่พัฒนาขึ้นมาควรมีการเข้ารหัสของการสื่อสารระหว่างเครื่องคอมพิวเตอร์แม่ข่ายและเครื่องคอมพิวเตอร์ลูกข่ายด้วยมาตรฐานของ HTTPS (SSL)

๒. ระบบงานสารสนเทศที่พัฒนาขึ้นมาต้องมีการพิสูจน์ หรือระบุตัวตนของผู้ใช้งาน และ บริหารจัดการรหัสผ่านสำหรับผู้ใช้งานได้

๓. ระบบงานสารสนเทศที่พัฒนาขึ้นมาต้องสามารถแบ่งแยกระดับของผู้ใช้งานได้

๔. ในการแบ่งแยกระดับของผู้ใช้งานต้องสามารถกำหนดสิทธิการเข้าใช้งานได้ชัดเจน

๕. เมื่อได้ทำการสร้างรายชื่อผู้ใช้งานไว้บนระบบสารสนเทศและไม่มีการ Login เลยตั้งแต่ได้ทำการสร้างไว้เป็นระยะเวลา ๑ เดือน ให้ทำการลบรายชื่อผู้ใช้งานนั้นออกจากระบบ

๖. มีการจัดเก็บการเข้าใช้งานระบบงาน (Log) โดยต้องมีรายละเอียดดังนี้เป็นอย่างน้อย

๖.๑. วันที่และเวลา

๖.๒. ผู้ใช้งาน

๖.๓. ระดับของผู้ใช้งาน

๖.๔. กิจกรรมที่ผู้ใช้งานกระทำ

๖.๕. ผลของการกระทำนั้น

๖.๖. รายละเอียดเพิ่มเติม (Comment หรือ Remark)

๗. การจัดเก็บบันทึกการใช้งานต้องไม่มีผู้ใช้งานใดสามารถแก้ไขบันทึกได้บนระบบงาน

๘. ระบบสามารถจัดทำรายงานจำนวนผู้ใช้งานบนระบบสารสนเทศ

๙. ระบบสามารถจัดทำรายงานผู้ที่พิสูจน์ตัวตนผิดและจำนวนครั้งที่ผิด

๑๐. กำหนดการตัดการเชื่อมต่อสำหรับผู้ใช้งานที่ไม่มีการดำเนินการกิจกรรมใด ๆ เป็นเวลาเกินกว่า ๑๕ นาที (Session Timeout) หรือตามความเหมาะสม

๑๑. กำหนดการเข้ารหัสข้อมูลในส่วนของข้อมูลที่มีความสำคัญ

๑๒. กำหนดการแบ่งแยกเครื่องทดสอบ และเครื่องที่มีการใช้งานจริงออกจากกัน

๑๓. กำหนดเครื่องทดสอบสามารถเข้าถึงได้จากภายในเพื่อทดสอบเท่านั้น

๑๔. กำหนดตรวจสอบการป้อนข้อมูลของผู้ใช้งาน (Input Validation) ให้ตรงกับความต้องการของระบบ

๑๕. กำหนดให้มีการเก็บรหัสของโปรแกรม (Source Code) ไว้ในที่ปลอดภัย ไม่ให้ผู้อื่นผู้ใดที่ไม่เกี่ยวข้องเข้าถึงได้

หมวด ๓

การบริหารการเปลี่ยนแปลง หรือนวัตกรรมของระบบสารสนเทศ (Change / Innovation System)

๑. การร่วมกันกำหนดโจทย์ เพื่อสร้างสิ่งประดิษฐ์ใด ๆ หรือเครื่องมือ ระบบ หรือชุดคำสั่งอื่นใด สำหรับเป็นแนวทาง วิธีการ ขบวนการ ในการแก้โจทย์ปัญหาข้างต้น ไม่ว่าจะเป็นการร่วมกันระหว่างบุคคลต่อบุคคล หน่วยงานต่อหน่วยงาน หรือบุคคลต่อหน่วยงาน รวมถึงเป็นการกระทำของบุคคลใด ๆ ด้วย ทั้งนี้ การกระทำข้างต้นต้องอยู่ภายใต้กำกับของผู้บังคับบัญชา

๒. การนำเสนอรายละเอียดการดำเนินการใด ๆ เพื่อปรับปรุง แก้ไข จัดการหรือเพิ่มเติมระบบหรือข้อมูลต่อระบบหรือชุดข้อมูลแก่คณะทำงานบริกรข้อมูล กรมควบคุมมลพิษ หรือหน่วยงานที่รับผิดชอบระบบงานหรืออุปกรณ์นั้น

๓. ให้มีการนำเสนอผลกระทบที่อาจจะเกิดขึ้น เมื่อมีการปรับปรุงแก้ไขหรือเพิ่มเติมระบบหรือข้อมูลเหล่านั้น พร้อมทั้งนำเสนอข้อแนวทางการแก้ไขเมื่อมีผลกระทบเกิดขึ้น

๔. จัดทำแผนสำรองในถอยกลับ (Roll back) เมื่อระบบไม่สามารถดำเนินการปรับปรุงแก้ไขหรือเพิ่มเติมระบบหรือข้อมูลได้

๕. มีการจัดเก็บบันทึก ข้อแก้ไข ปรับปรุงหรือเพิ่มเติมระบบหรือข้อมูลไว้เป็นลายลักษณ์อักษรให้ระบบสารสนเทศที่พัฒนาขึ้นมาต้องมีการเข้ารหัสของการสื่อสารระหว่างเครื่องคอมพิวเตอร์แม่ข่ายและเครื่องคอมพิวเตอร์ลูกข่ายด้วยมาตรฐานของ HTTPS (SSL)

หมวด ๔
การบริหารจัดการระบบฐานข้อมูล (Database Management)

๑. การตรวจสอบในส่วนของการ Update หรือ Service Pack หรือ Patch หรือ Hot Fix เวอร์ชั่นล่าสุดและให้นำมาติดตั้งสำหรับระบบฐานข้อมูลนั้น

๒. การปรับเปลี่ยน User Name และ Password ที่ได้มีการติดตั้งมาพร้อมกับระบบฐานข้อมูล

๓. ในส่วนของ User Name และ Password ต้องระบุและพิสูจน์ตัวตนของผู้ใช้งาน และ บริหารจัดการรหัสผ่านสำหรับเจ้าหน้าที่ดูแลเครื่องคอมพิวเตอร์แม่ข่ายและระบบเครือข่าย

๔. การทดสอบด้านความมั่นคงปลอดภัยด้วยการทำ Vulnerability Scanning หรือด้วยวิธีการอื่นใดตามที่กำหนด และดำเนินการปรับปรุงให้เสร็จเรียบร้อย ก่อนนำระบบเข้าใช้งานจริง

๕. ทดสอบการใช้งานของระบบฐานข้อมูล

๖. ดำเนินการสำรองข้อมูล รวมถึงค่า Configuration ไว้ก่อนการนำระบบไปใช้งาน

๗. เครื่องคอมพิวเตอร์แม่ข่ายที่ให้บริการระบบฐานข้อมูล ต้องติดตั้งอยู่ภายในกรมควบคุมมลพิษหรือสถานที่ที่กำหนด เท่านั้น

๘. เครื่องคอมพิวเตอร์แม่ข่ายที่ให้บริการระบบฐานข้อมูลต้องได้รับการควบคุมจาก Firewall และต้องอยู่ภายใต้โซนเครื่องคอมพิวเตอร์แม่ข่าย (Server) เท่านั้น

๙. การจัดทำคู่มือการติดตั้งเมื่อมีการติดตั้งระบบฐานข้อมูลที่ใหม่กว่าที่มีการใช้งานอยู่ พร้อมทั้งให้มีการฝึกอบรมการใช้งานระบบฐานข้อมูลนั้น หรือด้วยวิธีการอื่นใดตามที่กำหนด

๑๐.การ Shutdown / Reboot / Restart ของเครื่องคอมพิวเตอร์แม่ข่ายจะต้องให้เจ้าหน้าที่ที่ดูแลและรับผิดชอบเท่านั้นจึงจะสามารถดำเนินการได้

หมวด ๕
การบริหารจัดการ Web Server

๑. ต้องจัดทำ Web Server Security Checklist ขึ้นมา

๒. ให้มีการปรับปรุง Web Server Security Check List อย่างสม่ำเสมอและทันต่อสถานการณ์ปัจจุบันที่ได้มีการเปลี่ยนแปลงอยู่ตลอดเวลา

๓. การกำหนดเป็น Version ของเอกสาร Security Checklist เพื่อป้องกันการสับสนเมื่อนำไปใช้งาน

๔. ตรวจสอบการ Update หรือ Service Pack หรือ Patch หรือ Hot Fix เวอร์ชั่นล่าสุดและให้นำมาติดตั้ง

๕. ภายหลังที่มีการติดตั้ง Web Server จะต้องดำเนินการให้มีการเก็บบันทึกการเรียกใช้งานของ Web Server (Log) ทั้งในส่วนที่พบข้อผิดพลาดและส่วนของการเรียกใช้งานทั่วไป

๖. ให้ทำการทดสอบด้านความมั่นคงปลอดภัยด้วยการทำ Vulnerability Scanning และดำเนินการปรับปรุงให้เสร็จเรียบร้อย

๗. ทดสอบการใช้งานของ Web Server

๘. ดำเนินการสำรองข้อมูลไว้ก่อนการนำไปใช้งาน

๙. เครื่องคอมพิวเตอร์แม่ข่ายที่ให้บริการ Web Server ต้องติดตั้งอยู่ภายในกรมควบคุมมลพิษหรือสถานที่ที่กำหนดเท่านั้น

๑๐. เครื่องคอมพิวเตอร์แม่ข่ายที่ให้บริการ Web Server ต้องได้รับการควบคุมจาก Firewall และต้องอยู่ภายใต้โซนเครื่องคอมพิวเตอร์แม่ข่าย (Server) เท่านั้น

๑๑. จัดทำคู่มือการติดตั้งเมื่อมีการติดตั้ง Web Server ที่ใหม่กว่าที่มีการใช้งานอยู่ พร้อมทั้งให้มีการฝึกอบรมการใช้งาน Web Server นั้น

๑๒. การ Shutdown / Reboot / Restart ของเครื่องคอมพิวเตอร์แม่ข่ายจะต้องให้เจ้าหน้าที่ที่ดูแลและรับผิดชอบเท่านั้นจึงจะสามารถดำเนินการได้

หมวด ๖
นโยบายอื่น

๑. ข้อปฏิบัติหรือข้อห้ามตามหมวดนี้ให้เป็นไปตามนโยบายการใช้งานระบบสารสนเทศของกรมฯ ในเรื่องอื่น ๆ ที่เกี่ยวข้อง และกรมฯ กำหนดขึ้น

บทเฉพาะกาล

๑. การพัฒนาระบบสารสนเทศ สำหรับข้อ ๓ , ๖ และ ๙ กรมฯ จะดำเนินการเมื่อมีความพร้อม

หลักเกณฑ์การพัฒนาข้อมูลและสารสนเทศของกรมควบคุมมลพิษ
เรื่อง แนวปฏิบัติในการประเมินผลการกำกับดูแลข้อมูล (Data Governance Assessment Guideline)

เพื่อประโยชน์ในการดำเนินงานและสร้างความเข้าใจที่ถูกต้องตรงกัน สำหรับการบริหารจัดการและดำเนินการจัดทำของการพัฒนาฐานข้อมูลและระบบสารสนเทศของกรมควบคุมมลพิษ ตลอดจนการควบคุมและตรวจสอบการดำเนินงานที่เกี่ยวข้องกับข้อมูล ตั้งแต่การสร้าง การจัดเก็บ การประมวลผล การใช้ การเผยแพร่ จนถึงการทำลาย สำหรับตนเองหรือหน่วยงานที่เกี่ยวข้องต่อการพัฒนาและการปรับปรุงในการดำเนินงานที่เกี่ยวข้อง คณะทำงานบริกรข้อมูล กรมควบคุมมลพิษ จึงกำหนดแนวปฏิบัติในการประเมินผลการกำกับดูแลข้อมูลไว้ดังต่อไปนี้

หมวด ๑
การประเมินคุณภาพของข้อมูล (Data Quality Assessment)

๑. การประเมินผลต้องดำเนินการอย่างน้อย ๑ ครั้งต่อรอบการปฏิบัติงาน วิธีการทำงานหรือตามความเหมาะสมที่กำหนดของแต่ละขั้นตอนดำเนินงาน หรือตามนโยบายที่กำหนด

๒. การประเมินฯ ต้องครอบคลุมขั้นตอน วิธีการ หรือกระบวนการ อันเป็นสาระ หรือนัยสำคัญของวิธีการดำเนินการ เพื่อทราบประสิทธิภาพของวิธีทำงานนั้น ๆ เสมอ

๓. หน่วยงานต้องกำหนดผู้รับผิดชอบหรือเจ้าของข้อมูล สำหรับการดำเนินงานเกี่ยวข้องกับข้อมูล ตั้งแต่การสร้าง การจัดเก็บ การประมวลผล การใช้งาน การเผยแพร่ และการกำจัดทำลาย ตลอดจนจบกระบวนงานทั้งหมด รวมทั้งแนวทางการปรับปรุง หรือพัฒนาสำหรับการดำเนินงานด้วย (หากมี)

๔. หน้าที่ของผู้รับผิดชอบข้อมูลของระบบ

๔.๑. กำหนดขอบเขตของกระบวนการ หรือวิธีการ อันเป็นสาระที่ส่งผลกระทบอย่างเป็นนัยสำคัญต่อข้อมูลหรือระบบ

๔.๒. กำหนดลักษณะข้อมูล ตามเกณฑ์การจัดทำ Big Data ของกรมควบคุมมลพิษ ภายใต้คำแนะนำของกรอบการกำกับดูแลข้อมูล (Data Governance Framework)

๔.๓. ต้องจัดให้มีการดำเนินการตามข้อกำหนดข้างต้น พร้อมจัดทำหลักฐาน เอกสาร เพื่อยืนยันและตรวจสอบกระบวนการต่าง ๆ ได้เมื่อถูกร้องขอ

หมวด ๒
การประเมินความมั่นคงปลอดภัยของข้อมูล (Data Security Assessment)

๑. การบริหารจัดการข้อมูลองค์กร (Corporate Management)

๑.๑. ผู้ใช้งานต้องตระหนักและระมัดระวังต่อการใช้งานข้อมูล ไม่ว่าข้อมูลนั้นจะเป็นของกรมฯ หรือเป็นข้อมูลของบุคคลภายนอก

๑.๒. ข้อมูลทั้งหลายที่อยู่ภายในทรัพย์สินของกรมฯ ถือเป็นทรัพย์สินของกรมฯ ห้ามไม่ให้ทำการเผยแพร่ เปลี่ยนแปลง ทำซ้ำ หรือทำลาย โดยไม่ได้รับอนุญาตจากผู้บังคับบัญชา

๑.๓. ผู้ใช้งานมีส่วนร่วมในการดูแลรักษาและรับผิดชอบต่อข้อมูลของกรมฯ หรือข้อมูลของผู้รับบริการ หากเกิดการสูญหาย โดยนำไปใช้ในทางที่ผิด การเผยแพร่โดยไม่ได้รับอนุญาต ผู้ใช้งานต้องมีส่วนร่วมในการรับผิดชอบต่อความเสียหายนั้นด้วย

๑.๔. ผู้ใช้งานต้องป้องกัน ดูแล รักษาไว้ซึ่งความลับ ความถูกต้อง และความพร้อมใช้ของข้อมูล

๑.๕. ผู้ใช้งานมีสิทธิ์โดยชอบธรรมที่จะเก็บ รักษา ใช้งานและป้องกันข้อมูลส่วนบุคคลตามเห็นสมควร กรมฯ จะให้การสนับสนุนและเคารพต่อสิทธิ์ส่วนบุคคล และไม่อนุญาตให้บุคคลหนึ่งบุคคลใดทำการละเมิดต่อข้อมูลส่วนบุคคลโดยไม่ได้รับอนุญาตจากผู้ใช้งานที่ครอบครองข้อมูลนั้น ยกเว้นใน กรณีที่กรมฯ ต้องการตรวจสอบข้อมูลหรือ คาดว่าข้อมูลนั้นเกี่ยวข้องกับกรมฯ ซึ่งกรมฯ อาจแต่งตั้งให้ผู้ทำหน้าที่ตรวจสอบ ทำการตรวจสอบข้อมูลเหล่านั้นได้ตลอดเวลา โดยไม่ต้องแจ้งให้ผู้ใช้งานทราบ

๒. การบริหารจัดการระบบสารสนเทศ (IT Infrastructure Management)

๒.๑. ผู้ใช้งานมีสิทธิ์ที่จะพัฒนาโปรแกรมหรือฮาร์ดแวร์ใดๆ แต่ต้องไม่ดำเนินการดังนี้

๒.๑.๑. พัฒนาโปรแกรมหรือฮาร์ดแวร์ใด ๆ ที่จะทำลายกลไกรักษาความปลอดภัยระบบ รวมทั้งการกระทำในลักษณะเป็นการแอบใช้รหัสผ่าน การลักลอบทำสำเนาข้อมูลบุคคลอื่นหรือแกะรหัสผ่านของบุคคลอื่น

๒.๑.๒. พัฒนาโปรแกรมหรือฮาร์ดแวร์ใด ๆ ซึ่งทำให้ผู้ใช้มีสิทธิ์และลำดับความสำคัญในการครอบครองทรัพยากรระบบมากกว่าผู้ใช้อื่น

๒.๑.๓. พัฒนาโปรแกรมใดที่จะทำซ้ำตัวโปรแกรมหรือแฝงตัวโปรแกรมไปกับโปรแกรมอื่นในลักษณะเช่นเดียวกับหนอนหรือไวรัสคอมพิวเตอร์

๒.๑.๔. พัฒนาโปรแกรมหรือฮาร์ดแวร์ใด ๆ ที่จะทำลายระบบจำกัดสิทธิ์การใช้ (License) ซอฟต์แวร์

๒.๑.๕. นำเสนอข้อมูลที่ผิดกฎหมาย ละเมิดลิขสิทธิ์แสดงข้อความรูปภาพไม่เหมาะสม หรือขัดต่อศีลธรรมประเพณีอันดีงามของประเทศไทย กรณีที่ผู้ใช้สร้างเว็บเพจบนเครือข่ายคอมพิวเตอร์

๒.๒. ห้ามเปิดหรือใช้งาน (Run) โปรแกรมประเภท Peer-to-Peer หรือโปรแกรมที่มีความเสี่ยงในระดับเดียวกัน เช่น บิทเทอร์เรนท์ (Bit-torrent) อีมูล (e-mule) ฯลฯ เป็นต้น เว้นแต่จะได้รับอนุญาตจากผู้บังคับบัญชา

๒.๓. ห้ามเปิดหรือใช้งาน (Run) โปรแกรม ออนไลน์ทุกประเภท เพื่อความบันเทิง เช่น การดูหนัง ฟังเพลง เกมส์ เป็นต้น ในระหว่างเวลาปฏิบัติราชการ

๒.๔. ห้ามใช้ทรัพยากร ระบบสื่อสารทุกประเภท รวมถึงอุปกรณ์อื่นใดของกรมฯ ที่จัดเตรียมให้ เพื่อการเผยแพร่ ข้อมูล ข้อความ รูปภาพ หรือสิ่งอื่นใด ที่มีลักษณะขัดต่อศีลธรรม ความมั่นคงของประเทศ กฎหมาย หรือกระทบต่อภารกิจของกรมฯ หรือหน่วยงานอื่น ๆ

๒.๕. ห้ามใช้ทรัพยากร ระบบสื่อสารทุกประเภท รวมถึงอุปกรณ์อื่นใดของกรมฯ เพื่อการรบกวน ก่อให้เกิดความเสียหาย หรือใช้ในการโจรกรรมข้อมูล หรือสิ่งอื่นใดอันเป็นการขัดต่อกฎหมายและศีลธรรม หรือกระทบต่อภารกิจของกรมฯ หรือหน่วยงานอื่นๆ

๒.๖. ห้ามใช้ทรัพยากรทุกประเภทที่เป็นของกรมฯ เพื่อประโยชน์ทางการค้า

๒.๗. ห้ามกระทำการใด ๆ เพื่อการดักข้อมูล ไม่ว่าจะเป็นข้อความ ภาพ เสียง หรือสิ่งอื่นใดในเครือข่ายระบบสารสนเทศของกรมฯ โดยเด็ดขาด ไม่ว่าจะด้วยวิธีการใด ๆ ก็ตาม

๒.๘. ห้ามกระทำการรบกวน ทำลาย หรือทำให้ระบบสารสนเทศของกรมฯ ต้องหยุดชะงัก

๒.๙. ห้ามใช้ระบบสารสนเทศของกรมฯ เพื่อการควบคุมคอมพิวเตอร์หรือระบบสารสนเทศภายนอกโดยไม่ได้รับอนุญาตจากผู้มีอำนาจ

๒.๑๐. ห้ามกระทำการใด ๆ อันมีลักษณะเป็นการลักลอบใช้งานหรือรับรู้รหัสส่วนบุคคลของผู้อื่น ไม่ว่าจะเป็นกรณีใด ๆ เพื่อประโยชน์ในการเข้าถึงข้อมูล หรือเพื่อการใช้ทรัพยากรก็ตาม

๒.๑๑. ห้ามติดตั้งอุปกรณ์หรือกระทำการใดเพื่อให้สามารถเข้าถึงระบบสารสนเทศของกรมฯ โดยไม่ได้รับอนุญาตจากผู้มีอำนาจ

๓. การปฏิบัติตามกฎหมายและข้อบังคับ (Law and Compliance)

๓.๑. บรรดากฎหมายใด ๆ ที่ได้ประกาศใช้ในประเทศไทยรวมทั้งกฎระเบียบ ของกรมฯ ถือเป็นสิ่งสำคัญที่ผู้ใช้งานต้องตระหนักและปฏิบัติตามอย่างเคร่งครัด และไม่กระทำความผิดนั้น หากผู้ใช้งานกระทำผิดตามกฎหมายดังกล่าว ถือว่าความผิดนั้นเป็นความผิดส่วนบุคคล ซึ่งผู้ใช้งานจะต้องรับผิดชอบต่อความผิดที่เกิดขึ้นเอง

๓.๒. กฎหมายที่ประกาศใช้ และยังมีผลใช้บังคับในปัจจุบันและอาจประกาศใช้บังคับต่อไปในอนาคต ระเบียบและจรรยาบรรณด้านวิชาการถือรวมอยู่ในบรรดากฎหมายต่าง ๆ ด้วย

๔. ซอฟต์แวร์และลิขสิทธิ์ (Software Licensing and intellectual property)

๔.๑. กรมควบคุมมลพิษ ได้ให้ความสำคัญต่อเรื่องทรัพย์สินทางปัญญา ดังนั้นซอฟต์แวร์ที่กรมฯ อนุญาตให้ใช้งานหรือที่กรมฯ มีลิขสิทธิ์ ผู้ใช้งานสามารถขอใช้งานได้ตามหน้าที่ความจำเป็น และกรมฯ ห้ามไม่ให้ผู้ใช้งานทำการติดตั้งหรือใช้งานซอฟต์แวร์อื่นใดที่ไม่มีลิขสิทธิ์ หากมีการตรวจสอบพบความผิดฐานละเมิดลิขสิทธิ์กรมฯ ถือว่าเป็นความผิดส่วนบุคคล ผู้ใช้งานจะต้องรับผิดชอบแต่เพียงผู้เดียว

๔.๒. ซอฟต์แวร์ (Software) ที่กรมฯ ได้จัดเตรียมไว้ให้ผู้ใช้งาน ถือเป็นสิ่งจำเป็นต่อการทำงาน ห้ามมิให้ผู้ใช้งานทำการติดตั้ง ถอดถอน เปลี่ยนแปลง แก้ไข หรือทำสำเนาเพื่อนำไปใช้งานที่อื่น

๕. การป้องกันโปรแกรมไม่ประสงค์ดี (Preventing Mal-Ware)

๕.๑. คอมพิวเตอร์ของผู้ใช้งานต้องติดตั้งโปรแกรมป้องกันไวรัสคอมพิวเตอร์ (Antivirus) ตามที่กรมฯ ได้ประกาศให้ใช้ เว้นแต่คอมพิวเตอร์นั้นเป็นเครื่องเพื่อการศึกษา พัฒนา ระบบป้องกัน โดยต้องได้รับอนุญาตจากผู้บังคับบัญชา

๕.๒. บรรดาข้อมูล ไฟล์ ซอฟต์แวร์ หรือสิ่งอื่นใด ที่ได้รับจากผู้ใช้งานอื่นต้องได้รับการตรวจสอบไวรัสคอมพิวเตอร์และโปรแกรมไม่ประสงค์ดีก่อนนำมาใช้งานหรือเก็บบันทึกทุกครั้ง

๕.๓. ผู้ใช้งานต้องทำการปรับปรุงข้อมูล สำหรับตรวจสอบและปรับปรุงระบบปฏิบัติการ (Update patch) ให้ใหม่เสมอ เพื่อเป็นการป้องกันความเสียหายที่อาจเกิดขึ้น

๕.๔. ผู้ใช้งานต้องพึงระวังไวรัสและโปรแกรมไม่ประสงค์ดีตลอดเวลา รวมทั้งเมื่อพบสิ่งผิดปกติผู้ใช้งานต้องแจ้งเหตุแก่ผู้ดูแลระบบ

๕.๕. เมื่อผู้ใช้งานพบว่าเครื่องคอมพิวเตอร์ติดไวรัส ผู้ใช้งานต้องไม่เชื่อมต่อเครื่องคอมพิวเตอร์เข้าสู่เครือข่าย และ ต้องแจ้งแก่ผู้ดูแลระบบ

๕.๖. ห้ามลักลอบทำสำเนา เปลี่ยนแปลง ลบทิ้ง ซึ่งข้อมูล ข้อความ เอกสาร หรือสิ่งใด ๆ ที่เป็นทรัพย์สินของกรมฯ หรือของผู้อื่น โดยไม่ได้รับอนุญาตจากผู้มีอำนาจ

๕.๗. ห้ามทำการเผยแพร่ไวรัสคอมพิวเตอร์ มัลแวร์ หรือโปรแกรมอันตรายใด ๆ ที่อาจก่อให้เกิดความเสียหายมาสู่ทรัพย์สินของกรมฯ

๕.๘. ข้อปฏิบัติหรือข้อห้ามอื่น ๆ ตามหมวดนี้ให้เป็นไปตามนโยบายการป้องกันไวรัสคอมพิวเตอร์

๖. นโยบายอื่นๆ ที่กรมฯ กำหนดขึ้น

๖.๑. ข้อปฏิบัติหรือข้อห้ามตามหมวดนี้ให้เป็นไปตามนโยบายการใช้งานระบบสารสนเทศของกรมฯ ในเรื่องอื่น ๆ ที่เกี่ยวข้องและกรมฯ กำหนดขึ้น

<u>รายละเอียดแนบท้าย</u>

ก) ตารางตวจสอบข้อมูลหรือระบบ (Check list)

ข) ระดับความพร้อมของการกำกับดูแล (จาก Data Governance Framework กรอบการกำกับดูแลข้อมูล สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน))

ตารางตรวจสอบข้อมูลหรือระบบ (Check list)

ระดับความพร้อมของการกำกับดูแลและแนวทางการประเมินความพร้อมของการกำกับดูแลข้อมูล
(Data Governance Readiness Assessment)

การประเมินความพร้อมของการกำกับดูแลข้อมูลจะทำให้เราได้ทราบถึงสิ่งที่เราได้ดำเนินการแล้ว และสิ่งใดบ้างที่ควรจะดำเนินการต่อไป เพื่อปรับปรุงการดำเนินงานให้เกิดประสิทธิภาพสูงสุด ระดับความพร้อมของการกำกับดูแลข้อมูลถูกใช้เป็นเครื่องมือในการประเมินความพร้อมของการกำกับดูแลข้อมูล ซึ่งประกอบด้วยระดับชั้นจำนวน ๖ ระดับชั้น ดังต่อไปนี้

- ระดับ ๐ : None หมายถึง ไม่มีการกำกับดูแลข้อมูลหรือมีแต่ไม่ได้ดำเนินการอย่างเป็นทางการ นั่นคือ มีการดำเนินงานบางส่วนและไม่มีการประกาศให้ทราบอย่างเป็นทางการ

- ระดับ ๑ : Initial หมายถึง ไม่มีการกำหนดมาตรฐานของกระบวนการ นั่นคือ กระบวนการถูกกำหนดขึ้นมาเฉพาะกิจ (Ad-hoc) ทำให้แต่ละโครงการหรือบริการมีรูปแบบของกระบวนการที่แตกต่างกัน และอำนาจในการจัดการและกำกับดูแลข้อมูลส่วนใหญ่ถูกดำเนินการโดยฝ่ายเทคโนโลยีสารสนเทศทำให้การทำงานร่วมกันระหว่างด้านวิชาการและด้านเทคนิคหรือเทคโนโลยีสารสนเทศไม่สอดคล้องกัน

- ระดับ ๒ : Managed หมายถึง เริ่มมีการกำหนดมาตรฐานของกระบวนการเฉพาะแต่ละส่วนงานหรือบริการและมีการกำหนดบุคคลที่เกี่ยวข้องกับการกำกับติดตาม เช่น บริกรข้อมูลและเจ้าของข้อมูล

- ระดับ ๓ : Standardized หมายถึง กระบวนการถูกกำหนดเป็นมาตรฐานของหน่วยงาน มีการกำหนดส่วนงานกลางในการกำกับและติดตามข้อมูล ซึ่งมาจากบุคคลด้านธุรกิจและเทคโนโลยีสารสนเทศมีการบังคับใช้นโยบายข้อมูลครอบคลุมทั้งหน่วยงาน มีการติดตาม วิเคราะห์ และรายงานคุณภาพข้อมูลหรือความมั่นคงปลอดภัย

- ระดับ ๔ : Advanced หมายถึง กระบวนการถูกกำหนดเป็นมาตรฐานของหน่วยงาน มีการกำหนดส่วนงานกลางในการกำกับและติดตามข้อมูล ซึ่งมาจากบุคคลด้านธุรกิจและเทคโนโลยีสารสนเทศมีการบังคับใช้นโยบายข้อมูลครอบคลุมทั้งหน่วยงาน มีการติดตาม วิเคราะห์ และรายงานคุณภาพข้อมูลและความมั่นคงปลอดภัย

- ระดับ ๕ : Optimized หมายถึง มีการดำเนินการสอดคล้องกับระดับ ๔ วิเคราะห์สาเหตุของปัญหา (Root Cause) ประกอบไปด้วย ความไม่สอดคล้องในการปฏิบัติงานกับนโยบายข้อมูล (Non-Conformation) คุณภาพข้อมูลที่ต่ำ และความไม่คุ้มทุนในการบริหารจัดการข้อมูล ดำเนินการปรับปรุงกระบวนการ กฎเกณฑ์และนโยบายข้อมูล หรือโครงสร้างการกำกับดูแลข้อมูล เพื่อแก้ไขปัญหาที่พบจากผลการวิเคราะห์ และให้สอดคล้องกับความต้องการของผู้ที่เกี่ยวข้องและวัตถุประสงค์ที่เปลี่ยนไปของหน่วยงาน

ตารางแสดงระดับความพร้อมของการกำกับดูแลข้อมูล

ระดับ	โครงสร้างการกำกับดูแล	กระบวนการกำกับดูแล	นโยบายข้อมูลและการตรวจสอบ	การประเมินคุณภาพข้อมูลและความมั่นคงปลอดภัย	การวัดความคุ้มทุนและการปรับปรุงอย่างต่อเนื่อง
๐ : None	ไม่มีหรือมีแต่ไม่เป็นทางการ	ไม่มีหรือมีแต่ไม่เป็นทางการ	ไม่มีหรือมีแต่ไม่เป็นทางการ	ไม่มีหรือมีแต่ไม่เป็นทางการ	ไม่มีหรือมีแต่ไม่เป็นทางการ
๑ : Initial	มีการกำหนดผู้กำกับดูแลอย่างไม่เป็นทางการ	ไม่มีหรือมีแต่ไม่เป็นทางการ	ไม่มีหรือมีแต่ไม่เป็นทางการ	ไม่มีหรือมีแต่ไม่เป็นทางการ	ไม่มีหรือมีแต่ไม่เป็นทางการ
๒ : Managed	มีการกำหนดผู้กำกับดูแลในแต่ละส่วนงาน/บริการ	มีกระบวนการเป็นมาตรฐานส่วนงาน/บริการ	บังคับใช้ในส่วนงาน/บริการ	ไม่มีหรือมีแต่ไม่เป็นทางการ	ไม่มีหรือมีแต่ไม่เป็นทางการ
๓ : Standardized	มีส่วนงานกลางในการกำกับดูแล ซึ่งประกอบไปด้วยบุคคลด้านธุรกิจและเทคโนโลยีสารสนเทศ	มีกระบวนการเป็นมาตรฐานหน่วยงาน	บังคับใช้ทั้งหน่วยงาน	ประเมินคุณภาพข้อมูลหรือความมั่นคงปลอดภัย	ไม่มีหรือมีแต่ไม่เป็นทางการ
๔ : Advanced	มีส่วนงานกลางในการกำกับดูแล ซึ่งประกอบไปด้วยบุคคลด้านธุรกิจและเทคโนโลยีสารสนเทศ	มีกระบวนการเป็นมาตรฐานหน่วยงาน	บังคับใช้ทั้งหน่วยงาน	ประเมินคุณภาพข้อมูลหรือความมั่นคงปลอดภัย	ไม่มีหรือมีแต่ไม่เป็นทางการ
๕ : Optimized	มีส่วนงานกลางในการกำกับดูแล ซึ่งประกอบไปด้วยบุคคลด้านธุรกิจและเทคโนโลยีสารสนเทศ	มีกระบวนการเป็นมาตรฐานหน่วยงาน	บังคับใช้ทั้งหน่วยงาน	ประเมินคุณภาพข้อมูลหรือความมั่นคงปลอดภัย	มีการวัดความคุ้มทุนและปรับปรุงกระบวนการอย่างต่อเนื่อง