ประกาศสำนักงานบริหารหนี้สาธารณะ
เรื่อง นโยบายและแนวปฏิบัติธรรมาภิบาลข้อมูลของสำนักงานบริหารหนี้สาธารณะ พ.ศ. ๒๕๖๙

ด้วยพระราชบัญญัติการบริหารงานและการใช้บริการภาครัฐผ่านระบบดิจิทัล พ.ศ. ๒๕๖๒ กำหนดให้หน่วยงานของรัฐต้องจัดให้มีการบริหารงานภาครัฐและการจัดทำบริการสาธารณะให้เป็นไปด้วยความสะดวก รวดเร็ว มีประสิทธิภาพ ตอบสนองต่อการให้บริการ และอำนวยความสะดวกแก่ประชาชน รวมถึงกำหนดให้หน่วยงานของรัฐต้องจัดให้มีการบริหารจัดการบูรณาการข้อมูลภาครัฐ เพื่อให้การทำงานมีความสอดคล้องและเชื่อมโยงข้อมูลเข้าด้วยกันอย่างมั่นคงปลอดภัยและมีธรรมาภิบาล ประกอบกับคณะกรรมการพัฒนารัฐบาลดิจิทัลออกประกาศ เรื่อง มาตรฐานรัฐบาลดิจิทัลว่าด้วยกรอบธรรมาภิบาลข้อมูลภาครัฐ ฉบับปรับปรุง: แนวปฏิบัติ ณ วันที่ ๒๔ กรกฎาคม ๒๕๖๖ กำหนดให้มีธรรมาภิบาลข้อมูลภาครัฐเพื่อใช้เป็นหลักการและแนวทางการดำเนินงาน ดังนั้น เพื่อให้เป็นไปตามพระราชบัญญัติดังกล่าวสำนักงานบริหารหนี้สาธารณะ (สบน.) จึงกำหนดนโยบายการดำเนินงานด้านธรรมาภิบาลข้อมูลเพื่อใช้เป็นแนวทางในการปฏิบัติงาน ดังนี้

อาศัยอำนาจตามความในพระราชบัญญัติการบริหารงานและการให้บริการภาครัฐผ่านระบบดิจิทัล พ.ศ. ๒๕๖๒ มาตรา ๔ และมาตรา ๑๒ ประกอบกับประกาศคณะกรรมการพัฒนารัฐบาลดิจิทัล เรื่อง มาตรฐานรัฐบาลดิจิทัลว่าด้วยกรอบธรรมาภิบาลข้อมูลภาครัฐ ฉบับปรับปรุง: แนวปฏิบัติ ณ วันที่ ๒๔ กรกฎาคม ๒๕๖๖ ข้อ ๓ และข้อ ๔ กำหนดให้หน่วยงานของรัฐจัดทำธรรมาภิบาลข้อมูลภาครัฐในระดับหน่วยงานให้สอดคล้องกับธรรมาภิบาลข้อมูลภาครัฐ และประกอบกับมาตรา ๓๖ แห่งพระราชบัญญัติระเบียบบริหารราชการแผ่นดิน พ.ศ. ๒๕๓๔ และที่แก้ไขเพิ่มเติม จึงให้ยกเลิกประกาศสำนักงานบริหารหนี้สาธารณะ เรื่อง นโยบายและแนวปฏิบัติธรรมาภิบาลข้อมูลของสำนักงานบริหารหนี้สาธารณะ พ.ศ. ๒๕๖๘ และให้ใช้ประกาศฉบับนี้ จึงออกประกาศไว้ ดังต่อไปนี้

บทนำ

อำนาจหน้าที่ตามกฎกระทรวงแบ่งส่วนราชการ สบน. กระทรวงการคลัง พ.ศ. ๒๕๕๑ ให้ สบน. มีภารกิจเกี่ยวกับการบริหารหนี้สาธารณะตามกฎหมายว่าด้วยการบริหารหนี้สาธารณะ โดยการวางแผน กำกับ และดำเนินการก่อหนี้ ค้ำประกันและปรับโครงสร้างหนี้ของรัฐบาล หน่วยงานในกำกับดูแลของรัฐ องค์กรปกครองส่วนท้องถิ่น และรัฐวิสาหกิจ ซึ่งรวมทั้งการติดตามและประเมินผล เพื่อให้การบริหารหนี้สาธารณะเป็นไปอย่างมีประสิทธิภาพ และเสริมสร้างความยั่งยืนทางการคลังและการพัฒนาเศรษฐกิจ โดยให้มีอำนาจหน้าที่ดังต่อไปนี้

(๑) เสนอแนะนโยบายและหลักเกณฑ์ รวมทั้งการจัดทำแผนเกี่ยวกับการบริหารหนี้สาธารณะ

(๒) กำกับและดำเนินการเกี่ยวกับการบริหารหนี้สาธารณะซึ่งเป็นหนี้ที่หน่วยงานของรัฐหรือรัฐวิสาหกิจกู้ หรือหนี้ที่กระทรวงการคลังให้กู้ต่อหรือค้ำประกัน รวมทั้งกำกับดูแลการปฏิบัติตามสัญญาที่ได้ผูกพัน กฎหมายและข้อบังคับที่เกี่ยวข้องตลอดจนติดตามและประเมินผล

(๓) จัดทำงบชำระหนี้ของรัฐบาล รวมทั้งการบริหารและดำเนินการชำระหนี้

(๔) ประสานการทำความตกลงในระดับนโยบาย รวมทั้งการจัดทำแผนความช่วยเหลือทางการเงินและวิชาการกับแหล่งเงินกู้ต่างประเทศ

/(๕) ติดตาม ...

(๕) ติดตามภาวะตลาดเงินและตลาดทุน รวมทั้งเทคนิคในการบริหารหนี้สาธารณะและการพัฒนาตลาดตราสารหนี้ในประเทศ

(๖) ประสานงานและดำเนินการเกี่ยวกับการจัดอันดับความน่าเชื่อถือของประเทศ

(๗) ดำเนินการพัฒนาระบบสารสนเทศ รวมทั้งจัดทำข้อมูลสารสนเทศด้านหนี้สาธารณะ ระบบการบริหารความเสี่ยง และระบบเตือนภัยเกี่ยวกับหนี้สาธารณะ

(๘) พิจารณาความเหมาะสมของการระดมเงินสำหรับโครงการลงทุนของภาครัฐ

(๙) พัฒนาศูนย์ข้อมูลที่ปรึกษาให้เป็นศูนย์ในระดับภูมิภาค และส่งเสริมกิจการที่ปรึกษาไทยให้สามารถแข่งขันกับนานาประเทศ

(๑๐) ติดตามและประเมินผลการพัฒนาเศรษฐกิจและสังคม ฐานะการเงินการคลังของประเทศ ภาวะการค้าการลงทุน การเมืองในประเทศและนโยบายเศรษฐกิจของประเทศผู้นำทางเศรษฐกิจโลก

(๑๑) ปฏิบัติหน้าที่งานเลขานุการของคณะกรรมการนโยบายและกำกับการบริหารหนี้สาธารณะ

(๑๒) ปฏิบัติการอื่นใดตามที่กฎหมายกำหนดให้เป็นอำนาจหน้าที่ของสำนักงานหรือตามที่กระทรวงหรือคณะรัฐมนตรีมอบหมาย

ดังนั้น สบน. จึงได้จัดทำนโยบายและแนวปฏิบัติธรรมาภิบาลข้อมูลขึ้นเพื่อให้การบริหารจัดการข้อมูลของ สบน. มีธรรมาภิบาล สามารถบูรณาการ เชื่อมโยงและแลกเปลี่ยนข้อมูลระหว่างกันได้ โดยมีการกำหนดสิทธิ หน้าที่ ความรับผิดชอบในการบริหารจัดการข้อมูลของ สบน. เริ่มตั้งแต่การเก็บรวบรวม การใช้ การประมวลผล รวมถึงการเปิดเผยข้อมูลเป็นไปอย่างเหมาะสม มีประสิทธิภาพ คุณภาพ มั่นคงปลอดภัย สามารถป้องกันภัยคุกคามที่อาจจะเกิดขึ้นได้ เป็นไปตามพระราชบัญญัติการบริหารงานและการให้บริการภาครัฐผ่านระบบดิจิทัล พ.ศ. ๒๕๖๒

วัตถุประสงค์

๑. เพื่อให้การบริหารจัดการข้อมูลของ สบน. สอดคล้องกับพระราชบัญญัติการบริหารงานและการให้บริการภาครัฐผ่านระบบดิจิทัล พ.ศ. ๒๕๖๒ พระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ. ๒๕๔๐ พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ และเป็นไปตามกรอบธรรมาภิบาลข้อมูลภาครัฐ (Data Governance Framework for Government) ของสำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน) รวมถึงกฎหมาย ประกาศ และระเบียบอื่น ๆ ที่เกี่ยวข้อง

๒. เพื่อใช้เป็นกรอบและแนวปฏิบัติในการบริหารจัดการข้อมูลของ สบน. การรวบรวม การนำไปใช้ การประมวลผล และการเปิดเผยข้อมูล สำหรับผู้บริหาร บุคลากร และผู้ที่เกี่ยวข้อง

๓. เพื่อใช้เป็นแนวทางในการพัฒนาและปรับปรุงการบริหารจัดการข้อมูลให้เป็นไปตามกรอบธรรมาภิบาลข้อมูล รวมถึงการควบคุมคุณภาพของข้อมูลอย่างมีประสิทธิภาพ

ขอบเขต

นโยบายธรรมาภิบาลข้อมูลของ สบน. จัดทำขึ้นโดยคณะกรรมการพัฒนาระบบเทคโนโลยีดิจิทัลของ สบน. (คกก. DCIO) ประกอบกับนโยบายผู้บริหาร สบน. ที่มีการวางกรอบนโยบายให้เป็นไปตามประกาศคณะกรรมการพัฒนารัฐบาลดิจิทัล เรื่อง มาตรฐานรัฐบาลดิจิทัลว่าด้วยกรอบธรรมาภิบาลข้อมูลภาครัฐ ฉบับปรับปรุง: แนวปฏิบัติ ณ วันที่ ๒๔ กรกฎาคม ๒๕๖๖ โดยมีวัตถุประสงค์เพื่อกำหนดแนวทางการบริหารจัดการข้อมูลให้มีความโปร่งใส ตรวจสอบได้ ปลอดภัย และสอดคล้องกับกฎหมายและระเบียบที่เกี่ยวข้อง นโยบายฉบับนี้ครอบคลุมถึงหน่วยงานและบุคลากรที่มีส่วนเกี่ยวข้องในการบริหารจัดการข้อมูลของ สบน. ทั้งในระดับนโยบายและระดับปฏิบัติการ บุคคลหรือหน่วยงานที่อยู่ภายใต้ขอบเขตนโยบายจะต้องดำเนินงานและปฏิบัติตามนโยบายนี้

/คำนิยาม ...

คำนิยาม

“สำนักงาน” หมายถึง สำนักงานบริหารหนี้สาธารณะ

“คณะกรรมการ” หมายถึง คณะกรรมการพัฒนาระบบเทคโนโลยีดิจิทัลของสำนักงานหรือ คกก. DCIO

“ทีมบริกรข้อมูล” หมายถึง ทีมบริกรข้อมูลด้านหนี้สาธารณะ ด้านการพัฒนาตลาดตราสารหนี้ ด้านการประเมินผลโครงการลงทุนภาครัฐ ด้านการพัฒนาบุคลากร และด้านศูนย์ข้อมูลที่ปรึกษา

“บริกรข้อมูล” หมายถึง เจ้าหน้าที่ที่ได้รับแต่งตั้งจากคณะกรรมการ ให้ปฏิบัติหน้าที่ด้านธรรมาภิบาลข้อมูล และรายงานผลลัพธ์ต่อคณะกรรมการ

“บุคลากร” หมายถึง ข้าราชการ พนักงานราชการ ลูกจ้างและ/หรือ ผู้ปฏิบัติงานในสังกัดสำนักงาน

“หัวหน้าหน่วยงาน” หมายถึง ผู้อำนวยการ รองผู้อำนวยการ ที่ปรึกษา และหัวหน้าระดับสำนัก ศูนย์ กลุ่ม หรือผู้ที่ได้รับมอบหมาย

“ผู้รับผิดชอบที่เกี่ยวข้องกับข้อมูล” หมายถึง เจ้าหน้าที่ที่ทำหน้าที่ตรวจสอบดูแลข้อมูลโดยตรง ทำการทบทวนและอนุมัติการดำเนินการต่าง ๆ ที่เกี่ยวข้องกับข้อมูลตามธรรมาภิบาลข้อมูลตลอดวงจรชีวิตของข้อมูล รวมถึงการให้สิทธิในการเข้าถึงข้อมูลและจัดชั้นความลับของข้อมูล

“ธรรมาภิบาลข้อมูลภาครัฐ” หมายถึง การกำหนดสิทธิ หน้าที่ และความรับผิดชอบของผู้มีส่วนได้เสียในการบริหารจัดการข้อมูลภาครัฐทุกขั้นตอน เพื่อให้การได้มาและการนำข้อมูลไปใช้ของหน่วยงานภาครัฐถูกต้อง ครบถ้วน เป็นปัจจุบัน รักษาความเป็นส่วนบุคคล สามารถเชื่อมโยงแลกเปลี่ยนและบูรณาการระหว่างกันได้อย่างมีประสิทธิภาพและมั่นคงปลอดภัย โดยใช้ข้อมูลเป็นหลักในการบริหารงานภาครัฐและการบริการสาธารณะ

“บูรณาการข้อมูล” หมายถึง การจัดทำและจัดเก็บข้อมูลตั้งแต่สองแหล่งขึ้นไป ด้วยวิธีการเชื่อมโยงหรือแลกเปลี่ยนโดยขึ้นกับลักษณะการใช้งานเป็นสำคัญ เพื่อลดความซ้ำซ้อนและใช้ประโยชน์ข้อมูลร่วมกัน ตามความพร้อมของเจ้าของข้อมูลและภารกิจของสำนักงาน

“การบริหารจัดการข้อมูล” หมายถึง ขั้นตอนการสร้างข้อมูล การรวบรวมข้อมูล การจัดเก็บข้อมูล การจัดเก็บข้อมูลถาวร การทำลายข้อมูล การประมวลผลข้อมูล การใช้ข้อมูล การแลกเปลี่ยนข้อมูล การเชื่อมโยงข้อมูล และการเปิดเผยข้อมูลต่อสาธารณะ

“ข้อมูล” หมายถึง สิ่งที่สื่อความหมายให้รู้เรื่องราวข้อเท็จจริงหรือเรื่องอื่นใด ไม่ว่าการสื่อความหมายนั้นจะทำได้โดยสภาพของสิ่งนั้นเองหรือโดยผ่านวิธีการใด ๆ และไม่ว่าจะได้จัดทำไว้ในรูปของเอกสาร แฟ้ม รายงาน หนังสือ แผนผัง แผนที่ ภาพวาด ภาพถ่าย ภาพถ่ายดาวเทียม ฟิล์ม การบันทึกภาพหรือเสียง การบันทึกโดยเครื่องคอมพิวเตอร์ เครื่องมือตรวจวัด การสำรวจระยะไกล หรือวิธีอื่นใดที่ทำให้สิ่งที่บันทึกไว้ปรากฏได้

“ชุดข้อมูล” หมายถึง การนำข้อมูลจากหลายแหล่งมารวบรวม เพื่อจัดเป็นชุดข้อมูลให้ตรงตามลักษณะโครงสร้างของข้อมูล

“บัญชีข้อมูล” หมายถึง เอกสารแสดงรายการของชุดข้อมูล ที่จำแนกแยกแยะโดยการจัดกลุ่มหรือจัดประเภทข้อมูลที่อยู่ในความครอบครองหรือควบคุมของหน่วยงาน

“สารสนเทศ” หมายถึง ข้อมูล ข่าวสาร ในรูปแบบต่าง ๆ เช่น ตัวอักษร ตัวเลข สัญลักษณ์ รูปภาพ เสียง ที่ผ่านกระบวนการประมวลผล และบันทึกไว้อย่างเป็นระบบตามหลักวิชาการ ในสื่อประเภทต่าง ๆ

/เช่น ...

เช่น หนังสือ วารสาร หนังสือพิมพ์ วีดีโอ ซีดีรอม และฐานข้อมูลอิเล็กทรอนิกส์ เป็นต้น เพื่อนำออกเผยแพร่และใช้ประโยชน์

“ข้อมูลส่วนบุคคล” หมายถึง ข้อมูลเกี่ยวกับบุคคลซึ่งทำให้สามารถระบุตัวบุคคลนั้นได้ไม่ว่าทางตรงหรือทางอ้อม แต่ไม่รวมถึงข้อมูลของผู้ถึงแก่กรรมโดยเฉพาะ ตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒

“เมทาดาตา” หมายถึง ข้อมูลที่ใช้กำกับเพื่ออธิบายข้อมูลหรือกลุ่มของข้อมูล อธิบายรายละเอียดของข้อมูลหรือสารสนเทศ ทำให้ทราบรายละเอียดและคุณลักษณะข้อมูล

“วงจรชีวิตข้อมูล” หมายถึง ลำดับขั้นตอนของข้อมูล ตั้งแต่เริ่มสร้างข้อมูลไปจนถึงการทำลายข้อมูลตามกรอบธรรมาภิบาลข้อมูลภาครัฐ

“การจัดเก็บข้อมูล (Store)” หมายถึง การจัดเก็บข้อมูลที่เกิดจากกระบวนการสร้างหรือข้อมูลที่ได้จากการแลกเปลี่ยนกับหน่วยงานอื่น เพื่อให้มีระเบียบ ง่ายต่อการใช้งาน ไม่สูญหายหรือถูกทำลาย และทำให้ผู้ใช้งานสามารถประมวลผลข้อมูลต่าง ๆ ตามความต้องการได้อย่างรวดเร็ว ไม่ว่าจะเป็นการจัดเก็บลงแฟ้มข้อมูล (File) หรือระบบการจัดการฐานข้อมูล (Database Management System : DBMS)

“การประมวลผลและใช้ข้อมูล (Processing and Use)” หมายถึง การนำข้อมูลที่จัดเก็บมาประมวลผล เช่น การถ่ายโอนข้อมูล การเปลี่ยนรูปแบบการจัดเก็บข้อมูล การวิเคราะห์ข้อมูล การจัดทำรายงาน เพื่อนำข้อมูลเหล่านั้นมาใช้งานให้เกิดประโยชน์ตามวัตถุประสงค์ รวมถึงการสำรอง (Backup) ข้อมูล

“การเผยแพร่ข้อมูล (Disclosure)” หมายถึง การนำข้อมูลที่อยู่ในความครอบครองของสำนักงานตามช่องทางต่าง ๆ อย่างเหมาะสม เช่น การเปิดเผยข้อมูล (Open data) การแชร์ข้อมูล (Sharing) การกระจายข้อมูล (Dissemination) การควบคุมการเข้าถึง (Access Control) การแลกเปลี่ยนข้อมูลระหว่างหน่วยงาน (Exchange) และการกำหนดเงื่อนไขในการนำข้อมูลไปใช้ (Condition)

“การจัดเก็บข้อมูลถาวร (Archive)” หมายถึง การคัดลอกข้อมูลที่มีช่วงอายุเกินช่วงใช้งานหรือไม่ได้ใช้งานแล้ว เพื่อเก็บรักษาถาวรโดยที่ข้อมูลนั้นไม่มีการลบ ปรับปรุง หรือแก้ไขอีก และสามารถนำกลับไปใช้งานได้ใหม่เมื่อต้องการ

“การทำลายข้อมูล (Destroy)” หมายถึง การทำลายข้อมูลที่มีการจัดเก็บถาวรเป็นระยะเวลานานหรือเกินกว่าระยะเวลาที่กำหนด

/โครงสร้าง ...

โครงสร้างธรรมาภิบาลข้อมูล (Data Governance Structure)

บทบาท	ผู้รับผิดชอบ	ความรับผิดชอบ
ผู้บริหารข้อมูลระดับสูง (Chief Data Officer)	ที่ปรึกษา/รองผู้อำนวยการสำนักงานบริหารหนี้สาธารณะที่ได้รับแต่งตั้งให้เป็นผู้บริหารเทคโนโลยีสารสนเทศระดับสูง ระดับกรม ประจำสำนักงาน (DCIO)	ทำหน้าที่กำหนดนโยบายในการบริหารจัดการข้อมูลที่อยู่ในความครอบครองให้เป็นไปตามหลักธรรมาภิบาลข้อมูล (Data Governance) รวมถึงรับผิดชอบการบริหารจัดการธรรมาภิบาลข้อมูลและสารสนเทศทั้งหมดของสำนักงาน
คณะกรรมการพัฒนาระบบเทคโนโลยีดิจิทัลของสำนักงาน	ผู้อำนวยการสำนัก ศูนย์ กลุ่ม ที่ได้รับแต่งตั้ง	ทำหน้าที่ให้คำปรึกษา เสนอแนะการกำหนดและปรับปรุงนโยบายข้อมูล กรอบแนวทาง มาตรฐานข้อมูล และทิศทางการดำเนินงานเพื่อจัดทำธรรมาภิบาลข้อมูลให้สอดคล้องกับภารกิจของสำนักงาน ให้เป็นไปตามกรอบธรรมาภิบาลข้อมูลภาครัฐ รวมทั้งควบคุมการดำเนินงาน กำกับ ตรวจสอบ ประเมิน และรายงานผลเพื่อทบทวนและปรับปรุงให้มีความเหมาะสมอย่างต่อเนื่อง
ทีมบริกรข้อมูล (Data Stewards) ประกอบด้วย ๕ ทีม ๑. ทีมบริกรข้อมูลด้านหนี้สาธารณะ ๒. ทีมบริกรข้อมูลด้านพัฒนาตลาดตราสารหนี้ ๓. ทีมบริกรข้อมูลด้านการประเมินผลโครงการลงทุนภาครัฐ ๔. ทีมบริกรข้อมูลด้านการพัฒนาบุคลากร ๕. ทีมบริกรข้อมูลด้านศูนย์ข้อมูลที่ปรึกษา	ผู้แทนสำนัก ศูนย์ กลุ่ม ที่ได้รับมอบหมายให้เข้าร่วมทีมบริกรข้อมูล	ทำหน้าที่ร่างธรรมาภิบาลข้อมูล กำหนดนโยบาย จำแนกหมวดหมู่ มาตรการควบคุม และพัฒนาคุณภาพข้อมูล รวมถึงรับผิดชอบในการนิยามเมทาดาตา (Metadata) ให้ครบถ้วนตามแผนงานที่กำหนด ศึกษาและใช้เทคโนโลยีสารสนเทศที่เกี่ยวข้องกับการเปิดเผยข้อมูลตามหลักการจัดทำธรรมาภิบาลข้อมูลภาครัฐ ตรวจสอบความถูกต้องและปรับปรุงข้อมูลให้เป็นปัจจุบันอย่างต่อเนื่อง

/บทบาท ...

บทบาท	ผู้รับผิดชอบ	ความรับผิดชอบ
เจ้าของข้อมูล (Data Owner)	ผู้อำนวยการสำนัก ศูนย์ กลุ่ม หรือผู้ที่ได้รับมอบหมาย	ทำหน้าที่ตรวจสอบดูแลข้อมูลโดยตรง ทำการทบทวนและอนุมัติการดำเนินการต่าง ๆ ที่เกี่ยวข้องกับข้อมูลตามธรรมาภิบาลข้อมูลตลอดวงจรชีวิตของข้อมูล รวมถึงการให้สิทธิในการเข้าถึงข้อมูลและจัดชั้นความลับของข้อมูล
ผู้สร้างข้อมูล (Data Creators)	คณะกรรมการ คณะทำงาน หรือบุคลากรที่สร้างข้อมูล บันทึก แก้ไข ปรับปรุง หรือลบข้อมูล	ทำหน้าที่บันทึก แก้ไข ปรับปรุง หรือลบข้อมูลให้สอดคล้องกับโครงสร้างที่กำหนดไว้
ผู้ใช้ข้อมูล (Data Users)	บุคลากร หรือหน่วยงานทั้งภายในและภายนอกสำนักงาน	ทำหน้าที่นำข้อมูลไปใช้ หรือประมวลผลเพื่อดำเนินงานอื่นใดต่อไป

นโยบายธรรมาภิบาลข้อมูลของสำนักงานบริหารหนี้สาธารณะ

หมวด ๑ บททั่วไป

วัตถุประสงค์เพื่อกำหนดนโยบายข้อมูล กรอบแนวทาง มาตรฐานข้อมูล และทิศทางการดำเนินงานที่เกี่ยวข้องกับการบริหารจัดการข้อมูลของสำนักงาน ควบคุมการดำเนินงาน กำกับการตรวจสอบ ทบทวนและปรับปรุง ประเมินและรายงานผล ให้มีความเหมาะสมอย่างต่อเนื่อง เป็นไปตามกรอบธรรมาภิบาลข้อมูลภาครัฐ สอดคล้องกับภารกิจของสำนักงาน รวมทั้งสอดคล้องกับกฎหมายและระเบียบต่าง ๆ ที่เกี่ยวข้องต่อไปนี้เป็นอย่างน้อย ได้แก่

รัฐธรรมนูญ

- รัฐธรรมนูญแห่งราชอาณาจักรไทย พุทธศักราช ๒๕๖๐

พระราชบัญญัติ

- พระราชบัญญัติการบริหารหนี้สาธารณะ พ.ศ. ๒๕๔๘ และที่แก้ไขเพิ่มเติม
- พระราชบัญญัติวินัยการเงินการคลังของรัฐ พ.ศ. ๒๕๖๑
- พระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ. ๒๕๔๐
- พระราชบัญญัติการบริหารงานและการให้บริการภาครัฐผ่านระบบดิจิทัล พ.ศ. ๒๕๖๒
- พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒
- พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒
- พระราชบัญญัติการปฏิบัติราชการทางอิเล็กทรอนิกส์ พ.ศ. ๒๕๖๕

กฎกระทรวง

- กฎกระทรวงแบ่งส่วนราชการสำนักงานบริหารหนี้สาธารณะ กระทรวงการคลัง พ.ศ. ๒๕๕๑

/ระเบียบ ...

ระเบียบ

- ระเบียบคณะกรรมการนโยบายและกำกับการบริหารหนี้สาธารณะว่าด้วยหลักเกณฑ์การบริหารหนี้สาธารณะ พ.ศ. ๒๕๖๑

- ระเบียบสำนักงานบริหารหนี้สาธารณะว่าด้วยหลักเกณฑ์และวิธีการจ้างบริษัทจัดอันดับความน่าเชื่อถือเพื่อให้ดำเนินการจัดอันดับความน่าเชื่อถือของประเทศไทย พ.ศ. ๒๕๖๒

- ระเบียบสำนักนายกรัฐมนตรีว่าด้วยงานสารบรรณ พ.ศ. ๒๕๒๖ และที่แก้ไขเพิ่มเติม

- ระเบียบว่าด้วยการรักษาความลับของทางราชการ พ.ศ. ๒๕๔๔ และที่แก้ไขเพิ่มเติม

- ระเบียบสำนักนายกรัฐมนตรีว่าด้วยการรักษาความปลอดภัยแห่งชาติ พ.ศ. ๒๕๕๒

ประกาศ

- ประกาศคณะกรรมการนโยบายการเงินการคลังของรัฐ เรื่อง หลักเกณฑ์การรายงานสถานะหนี้สาธารณะ หนี้ภาครัฐ และความเสี่ยงทางการคลัง พ.ศ. ๒๕๖๑

- ประกาศกระทรวงการคลัง เรื่อง กำหนดหลักเกณฑ์และวิธีการในการจัดทำแผนการกู้เงินและบริหารหนี้เงินกู้ และการรายงานการกู้เงินและสถานะหนี้เงินกู้คงค้างของหน่วยงานของรัฐ

- ประกาศสำนักงานบริหารหนี้สาธารณะ เรื่อง การกำหนดจรรยาบรรณที่ปรึกษา วิธีการและขั้นตอนการขึ้นทะเบียนที่ปรึกษา และที่แก้ไขเพิ่มเติม

- ประกาศสำนักงานบริหารหนี้สาธารณะ เรื่อง นโยบายการคุ้มครองข้อมูลส่วนบุคคล

- ประกาศสำนักงานบริหารหนี้สาธารณะ เรื่อง นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศและการคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๗

- ประกาศคณะกรรมการพัฒนารัฐบาลดิจิทัล เรื่อง มาตรฐานรัฐบาลดิจิทัลว่าด้วยกรอบธรรมาภิบาลข้อมูลภาครัฐ ฉบับปรับปรุง: แนวปฏิบัติ (มรด. ๖ : ๒๕๖๖)

- ประกาศคณะกรรมการพัฒนารัฐบาลดิจิทัล เรื่อง มาตรฐานรัฐบาลดิจิทัลว่าด้วยข้อเสนอแนะสำหรับการจัดทำนโยบายและแนวปฏิบัติการบริหารจัดการข้อมูล (มรด. ๔-๑ : ๒๕๖๕ และ มรด. ๔-๒ : ๒๕๖๕)

- ประกาศคณะกรรมการพัฒนารัฐบาลดิจิทัล เรื่อง มาตรฐานรัฐบาลดิจิทัลว่าด้วยข้อเสนอแนะสำหรับแนวทางการจัดทำบัญชีข้อมูลภาครัฐและแนวทางการลงทะเบียนบัญชีข้อมูลภาครัฐ (มรด. ๓-๑ : ๒๕๖๕)

- ประกาศคณะกรรมการพัฒนารัฐบาลดิจิทัล เรื่อง มาตรฐานของสำนักงานพัฒนารัฐบาลดิจิทัลว่าด้วยหลักเกณฑ์การจัดระดับชั้นและการแบ่งปันข้อมูลภาครัฐ (มสพร. ๘-๒๕๖๕)

- ประกาศคณะกรรมการพัฒนารัฐบาลดิจิทัล เรื่อง มาตรฐานรัฐบาลดิจิทัลว่าด้วยหลักเกณฑ์การประเมินคุณภาพข้อมูลสำหรับหน่วยงานภาครัฐ (มรด. ๕ : ๒๕๖๕)

โดยมีรายละเอียด ดังนี้

๑. นโยบายธรรมาภิบาลข้อมูลต้องจัดทำเป็นลายลักษณ์อักษร และต้องได้รับการอนุมัติเพื่อประกาศใช้และถือปฏิบัติทั่วทั้งสำนักงาน โดยให้มีผลบังคับใช้กับบุคลากรในทุกระดับชั้นของสำนักงาน

๒. ผู้อำนวยการสำนักงานบริหารหนี้สาธารณะ หรือผู้ที่ได้รับมอบอำนาจ มีอำนาจกำหนดบทบาทหน้าที่และความรับผิดชอบตามโครงสร้างธรรมาภิบาลข้อมูลภาครัฐ

๓. กำหนดให้ผู้อำนวยการสำนัก ศูนย์ กลุ่ม หรือผู้ที่ได้รับมอบหมาย เป็นผู้กำหนดสิทธิการบริหารจัดการข้อมูลที่อยู่ในขอบเขตความรับผิดชอบของตน

/๔. กำหนด ...

๔. กำหนดให้มีการวัดผลการดำเนินการและความสำเร็จของธรรมาภิบาลข้อมูลภาครัฐ โดยมีการวัดผลอย่างน้อยในเรื่องดังต่อไปนี้ (๑) การประเมินความพร้อมธรรมาภิบาลข้อมูลภาครัฐ (๒) การประเมินคุณภาพข้อมูลและ (๓) การประเมินความมั่นคงปลอดภัยของข้อมูล

๕. กำหนดให้มีการติดตาม และรายงานผลการดำเนินงาน อย่างน้อยปีละ ๑ ครั้ง เพื่อนำมาปรับปรุงการบริหารจัดการข้อมูลให้มีประสิทธิภาพมากขึ้น

๖. กำหนดให้มีการรักษาความมั่นคงปลอดภัยของข้อมูล เพื่อป้องกันการละเมิด การเข้าถึง การสูญหาย การทำลาย หรือการเปลี่ยนแปลงข้อมูล โดยปราศจากอำนาจโดยมิชอบ หรือโดยมิได้รับอนุญาต

๗. กำหนดให้มีมาตรการ วิธีการ และแนวปฏิบัติในการคุ้มครองข้อมูลข่าวสารส่วนบุคคล ข้อมูลส่วนบุคคล และข้อมูลในความรับผิดชอบของสำนักงาน

๘. กำหนดให้มีการจัดทำสถาปัตยกรรมองค์กรและพัฒนาระบบการบริหารข้อมูลให้เป็นไปตามกรอบสถาปัตยกรรมองค์กร

๙. กำหนดให้มีการจัดทำระบบบัญชีข้อมูลตามกรอบมาตรฐานการจัดทำบัญชีข้อมูลภาครัฐ

๑๐. กำหนดให้มีแนวปฏิบัติเพื่อสนับสนุนการปฏิบัติงานให้สอดคล้องตามนโยบายข้อมูลและทบทวนแนวปฏิบัติให้เป็นตามพระราชบัญญัติและระเบียบที่บังคับใช้

๑๑. กำหนดให้มีการเผยแพร่ประชาสัมพันธ์นโยบายข้อมูลให้แก่บุคคลหรือหน่วยงานที่เกี่ยวข้องทั้งภายในและภายนอก รวมทั้งผู้มีส่วนได้ส่วนเสีย เพื่อให้มีความรู้ความเข้าใจต่อการปฏิบัติตามนโยบายข้อมูล

๑๒. กำหนดให้มีการตรวจสอบการปฏิบัติตามนโยบายข้อมูล โดยผู้ตรวจประเมินของสำนักงาน และติดตามผลการประเมินเพื่อปรับปรุง ป้องกัน หรือแก้ไขปัญหาที่พบอย่างต่อเนื่อง

๑๓. กำหนดให้มีการทบทวนนโยบายธรรมาภิบาลข้อมูลภาครัฐในทุก ๑ ปี และการทบทวนการจัดระดับชั้นของข้อมูลต้องบรรจุในวาระการประชุมคณะกรรมการ อย่างน้อยปีละ ๒ ครั้ง หรือเมื่อมีการเปลี่ยนแปลงที่สำคัญ และปรับปรุงอย่างต่อเนื่อง

๑๔. กำหนดให้มีมาตรฐานหรือวิธีปฏิบัติที่เกี่ยวกับข้อมูล ได้แก่ มาตรฐานการจัดชั้นความลับของข้อมูล เพื่อจัดลำดับความสำคัญของข้อมูลให้มีความมั่นคงปลอดภัยสารสนเทศอย่างเหมาะสม

๑๕. กำหนดให้แจ้งความมีอยู่และรายละเอียดของข้อมูลที่สำคัญ เช่น คำอธิบายข้อมูลหรือเมทาดาตา ชุดข้อมูล และการจัดชั้นความลับข้อมูล เป็นต้น ให้แก่ผู้รับผิดชอบตามโครงสร้างธรรมาภิบาลข้อมูลภาครัฐทราบ และดำเนินการตามกระบวนการธรรมาภิบาลข้อมูลภาครัฐ

๑๖. กำหนดสภาพแวดล้อมของการจัดเก็บข้อมูลที่เอื้อต่อการรักษาความมั่นคงปลอดภัยและคุณภาพของข้อมูล

๑๗. จัดให้มีทรัพยากรด้านงบประมาณ ทรัพยากรบุคคล และการบริหารจัดการเทคโนโลยีที่เพียงพอต่อการบริหารจัดการข้อมูล และส่งเสริมการนำระบบเทคโนโลยีสารสนเทศหรือระบบอัตโนมัติมาใช้เพื่อการเปิดเผยข้อมูลตามหลักการจัดทำธรรมาภิบาลข้อมูลภาครัฐ

๑๘. สนับสนุนให้มีการฝึกอบรมเพื่อสร้างความตระหนักถึงธรรมาภิบาลข้อมูลภาครัฐและการบริหารจัดการข้อมูล โดยให้ครอบคลุมทุกกระบวนการของการบริหารจัดการและวงจรชีวิตของข้อมูล

/หมวด ๒ ...

หมวด ๒ การสร้างและการรวบรวมข้อมูล

วัตถุประสงค์เพื่อกำหนดนโยบายในการสร้างและการรวบรวมข้อมูลอย่างมีคุณภาพ โดยมีรายละเอียด ดังนี้

๑. การสร้างและการรวบรวมข้อมูลต้องมีการรักษาความมั่นคงปลอดภัย และความเป็นส่วนบุคคลของข้อมูล และปฏิบัติตามแนวปฏิบัติในการปกป้องข้อมูลที่ระบุตัวบุคคล และแนวปฏิบัติในด้านความมั่นคงปลอดภัย โดยให้เป็นไปตามบทบัญญัติของกฎหมาย

๒. เจ้าของข้อมูลต้องกำหนดชั้นความลับของข้อมูลที่สร้างและ/หรือเก็บรวบรวม

๓. เจ้าของข้อมูลต้องจัดให้มีเมทาดาตา สำหรับชุดข้อมูลที่มีการสร้างและ/หรือเก็บรวบรวม ให้มีความถูกต้อง ครบถ้วน และเป็นปัจจุบัน

หมวด ๓ การจัดเก็บข้อมูลและทำลายข้อมูล

วัตถุประสงค์เพื่อกำหนดนโยบายในการจัดเก็บข้อมูลและทำลายข้อมูลอย่างมีคุณภาพ มีการรักษาความปลอดภัยของข้อมูล โดยมีรายละเอียด ดังนี้

๑. การกำหนดชั้นความลับของข้อมูล ให้ดำเนินการตามระเบียบว่าด้วยการรักษาความลับของทางราชการ พ.ศ. ๒๕๔๔ และที่แก้ไขเพิ่มเติม

๒. จัดเก็บให้สอดคล้องกับแนวทางหรือมาตรฐานการจัดชั้นความลับของข้อมูลที่กำหนดไว้ เพื่อให้ข้อมูลมีความมั่นคงปลอดภัย และรักษาคุณภาพของข้อมูล

๓. กำหนดสิทธิการเข้าถึงข้อมูลและเครื่องมือที่ใช้ในการเข้าถึงข้อมูล

๔. จัดเก็บข้อมูลให้สอดคล้องกับกระบวนงานและวัตถุประสงค์ในการดำเนินงาน โดยข้อมูลต้องมีความถูกต้อง สมบูรณ์ และเป็นปัจจุบัน โดยจัดทำเมทาดาตาสำหรับชุดข้อมูลที่มีการจัดเก็บ

๕. การเก็บรวบรวมข้อมูลส่วนบุคคล ให้เก็บรวบรวมได้เท่าที่จำเป็น และควรกำหนดระยะเวลาในการเก็บรวบรวมไว้ด้วย ทั้งนี้ ให้เป็นไปตามกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล

๖. ในกรณีที่เจ้าของข้อมูลขอใช้สิทธิตามกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล ผู้ควบคุมข้อมูลส่วนบุคคลต้องดำเนินการตามคำขอใช้สิทธิของเจ้าของข้อมูลโดยไม่ชักช้า

๗. กำหนดแนวปฏิบัติในการทำลายข้อมูลเมื่อข้อมูลไม่มีการใช้งานหรือมีการจัดเก็บเกินระยะเวลาที่กำหนด แต่ควรมีการเก็บรักษาเมทาดาตาของข้อมูลที่ทำลายไว้เพื่อใช้สำหรับการตรวจสอบ

๘. สร้างความรู้ความเข้าใจในการจัดเก็บและทำลายข้อมูลให้แก่ผู้เกี่ยวข้องทั้งภายในและภายนอกสำนักงาน

หมวด ๔ การประมวลผลข้อมูลและการใช้ข้อมูล

วัตถุประสงค์เพื่อกำหนดนโยบายในการประมวลผลข้อมูลและการใช้ข้อมูล ให้ได้ข้อมูลที่มีประสิทธิภาพ ถูกต้อง ตรงตามวัตถุประสงค์ของการใช้ข้อมูล โดยมีรายละเอียด ดังนี้

๑. กำหนดแนวปฏิบัติและมาตรฐานของการประมวลผลข้อมูล

๒. การประมวลผลข้อมูลที่เป็นความลับให้เป็นไปตามระเบียบว่าด้วยการรักษาความลับของทางราชการ พ.ศ. ๒๕๕๔ และที่แก้ไขเพิ่มเติม

๓. การประมวลผลข้อมูลที่เป็นข้อมูลข่าวสารส่วนบุคคล ข้อมูลส่วนบุคคล ให้เป็นไปตามขอบเขต เงื่อนไข หรือวัตถุประสงค์ ตามกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล

/๔. จัดทำ ...

๔. จัดทำเมทาดาตาสำหรับข้อมูลที่จัดเก็บให้อยู่ในระบบฐานข้อมูล

๕. ต้องบันทึกประวัติการประมวลผลและการใช้ข้อมูล (Log File) เพื่อให้สามารถตรวจสอบย้อนกลับได้

๖. สร้างความตระหนักรู้ของผู้ใช้ข้อมูล รวมถึงความรับผิดชอบต่อผลกระทบจากการนำข้อมูลไปใช้ การเข้าถึงและใช้ข้อมูลตามความจำเป็นในการปฏิบัติงาน โดยไม่แสวงหาผลประโยชน์ส่วนตัว หรือเพื่อวัตถุประสงค์อื่นที่ไม่เหมาะสม

หมวด ๕ การเปิดเผยข้อมูล

วัตถุประสงค์เพื่อกำหนดนโยบายในการเปิดเผยข้อมูล เพื่อให้สามารถเปิดเผยข้อมูลได้อย่างถูกต้อง ตรงตามวัตถุประสงค์ของการให้นำข้อมูลไปใช้ประโยชน์ โดยมีรายละเอียด ดังนี้

๑. ห้ามเปิดเผยข้อมูลที่ขัดต่อกฎหมาย ระเบียบ ข้อบังคับ คำสั่ง นโยบาย และแนวปฏิบัติ ไม่ว่าข้อมูลจะอยู่ในรูปแบบใดหรือสถานที่ใดก็ตาม

๒. ต้องได้รับการอนุญาตจากเจ้าของข้อมูลก่อนการเปิดเผยข้อมูล

๓. ให้มีการระบุช่องทางการเปิดเผยข้อมูลที่เข้าถึงและนำไปใช้ได้ง่าย

๔. ให้มีการเปิดเผยเมทาดาตาควบคู่ไปกับข้อมูลที่มีการเปิดเผย

๕. ต้องตรวจสอบได้ว่าการเปิดเผยข้อมูลได้ดำเนินการอย่างเหมาะสมหรือเป็นไปตามแนวทางหรือแนวปฏิบัติที่กำหนดไว้ เพื่อให้ได้ข้อมูลที่มีคุณภาพ และรักษาคุณภาพของข้อมูล

หมวด ๖ การแลกเปลี่ยนและการเชื่อมโยง

วัตถุประสงค์เพื่อกำหนดนโยบายในการแลกเปลี่ยนและการเชื่อมโยงข้อมูลระหว่างหน่วยงานทั้งภายในและภายนอก ให้มีความมั่นคงปลอดภัย และข้อมูลมีคุณภาพ สามารถนำไปใช้ประโยชน์ได้อย่างมีประสิทธิภาพ โดยมีรายละเอียด ดังนี้

๑. กำหนดแนวปฏิบัติด้านการรักษาความมั่นคงปลอดภัยสารสนเทศ โดยรวมถึงคุณภาพข้อมูล และผู้ประสานงานหรือศูนย์ติดต่อ (Contact Center)

๒. กำหนดกระบวนการในการแลกเปลี่ยนข้อมูล กระบวนการเชื่อมโยงข้อมูล การรวบรวมข้อมูลส่วนบุคคล โดยนำมาตรฐานสากลมาประยุกต์ใช้งาน

๓. กำหนดเมทาดาตาของชุดข้อมูลที่ต้องการแลกเปลี่ยนและเชื่อมโยงข้อมูลให้ครบถ้วน

๔. จัดทำสัญญาอนุญาตหรือข้อตกลงในการแลกเปลี่ยนและเชื่อมโยงข้อมูล และ/หรือการนำข้อมูลไปใช้ รวมถึงข้อตกลงยินยอมให้ส่งข้อมูลส่วนบุคคล

๕. กำหนดเทคโนโลยีและมาตรฐานทางเทคนิคที่ใช้ในการแลกเปลี่ยนและเชื่อมโยงข้อมูลและการรวบรวมข้อมูลส่วนบุคคล

๖. ต้องบันทึกรายละเอียดและจัดเก็บข้อมูลการดำเนินงานที่เกิดขึ้นในแต่ละครั้งที่มีการแลกเปลี่ยนและเชื่อมโยงข้อมูล การรวบรวมข้อมูลส่วนบุคคล (Log File) ระหว่างหน่วยงาน เพื่อการตรวจสอบย้อนกลับ

๗. ต้องตรวจสอบได้ว่าการแลกเปลี่ยนและเชื่อมโยงข้อมูล และการรวบรวมข้อมูลส่วนบุคคลได้ดำเนินการอย่างเหมาะสมหรือเป็นไปตามแนวปฏิบัติและมาตรฐานที่กำหนด

/แนวปฏิบัติ ...

แนวปฏิบัติธรรมาภิบาลข้อมูลของสำนักงานบริหารหนี้สาธารณะ

หมวด ๑ วงจรชีวิตข้อมูล (Data Life Cycle)

กระบวนการธรรมาภิบาลข้อมูลเป็นขั้นตอนที่ใช้สำหรับกำกับดูแลการดำเนินการใด ๆ ต่อข้อมูล ให้เป็นไปตามกฎ ระเบียบ ข้อบังคับ หรือนโยบายที่เกี่ยวข้องกับข้อมูล ขั้นตอนการจัดทำธรรมาภิบาลข้อมูลเริ่มตั้งแต่การวางแผนไปจนถึงการปรับปรุงอย่างสม่ำเสมอ เพื่อให้ข้อมูลมีความถูกต้องและเป็นปัจจุบัน โดยมีรายละเอียดและแนวทางปฏิบัติ ดังนี้

๑. การสร้างข้อมูล (Data Creation) เป็นการสร้างข้อมูลขึ้นมาใหม่ หรือปรับปรุงข้อมูลเดิม โดยวิธีการบันทึกข้อมูลด้วยบุคคลหรือบันทึกด้วยอุปกรณ์อิเล็กทรอนิกส์ การรับข้อมูลจากหน่วยงานอื่น เพื่อนำมาจัดเก็บทั้งข้อมูลที่เป็นกระดาษ และข้อมูลที่เป็นอิเล็กทรอนิกส์ทุกประเภท ให้บุคลากรต้องปฏิบัติตามกฎหมายว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ รวมทั้งกฎหมายอื่น ๆ ที่เกี่ยวข้อง โดยมีรายละเอียด ดังนี้

๑.๑ การสร้างข้อมูลต้องมีความถูกต้อง ครบถ้วน เป็นปัจจุบัน ตรงตามความต้องการของผู้ใช้

๑.๒ หน่วยงานที่สร้างข้อมูล ต้องเป็นผู้ตรวจสอบและบันทึกข้อมูลให้ถูกต้อง ครบถ้วน ตรงกับข้อเท็จจริง รวมถึงต้องสร้างจิตสำนึกและความรับผิดชอบต่อข้อมูลที่สร้างขึ้น โดยไม่สร้างข้อมูลอันเป็นเท็จ

๑.๓ ข้อมูลที่สร้างขึ้นแล้ว ต้องกำหนดมาตรฐานการจัดเก็บข้อมูล

๒. การจัดเก็บข้อมูล (Data Store) เป็นการจัดเก็บข้อมูลที่เกิดจากกระบวนการสร้างหรือข้อมูลที่ได้จากการเชื่อมโยงและ/หรือแลกเปลี่ยนกับหน่วยงานอื่น ไม่ว่าจะจัดเก็บลงในแฟ้มข้อมูลหรือระบบการจัดการฐานข้อมูล (Database Management System - DBMS) เพื่อให้เกิดความมีระเบียบต่อการใช้งานข้อมูลไม่สูญหายหรือถูกทำลาย และช่วยให้ผู้ใช้งานสามารถประมวลผลข้อมูลตามความต้องการได้อย่างรวดเร็วการจัดเก็บข้อมูล หมายความรวมถึง ข้อมูลทั้งที่เป็นกระดาษ และข้อมูลที่เป็นอิเล็กทรอนิกส์ทุกประเภท ไม่ว่าจัดเก็บแฟ้มข้อมูลดิจิทัลทั่วไป หรือแฟ้มข้อมูลที่ผ่านการประมวลผล หรือแฟ้มข้อมูลอื่น กล่าวคือ

๒.๑ ต้องจัดเก็บข้อมูลตามหมวดหมู่ โดยมีการกำหนดหมวดหมู่ของข้อมูล ดังนี้

๒.๑.๑ ข้อมูลส่วนบุคคล หมายถึง ข้อมูลเกี่ยวกับบุคคลซึ่งทำให้สามารถระบุตัวบุคคลนั้นได้ ไม่ว่าทางตรงหรือทางอ้อม แต่ไม่รวมถึงข้อมูลของผู้ถึงแก่กรรม

๒.๑.๒ ข้อมูลความมั่นคง หมายถึง ข้อมูลข่าวสารเกี่ยวกับความมั่นคงของประเทศที่อยู่ในความครอบครองหรือความควบคุมดูแลของสำนักงาน ที่ไม่สามารถรู้หรือไม่สามารถเข้าถึงได้โดยทั่วไป ซึ่งหากเปิดเผยทั้งหมดหรือเพียงบางส่วนจะส่งผลให้ประเทศต้องเผชิญกับภัยคุกคามต่อเอกราช อธิปไตยอันมีพระมหากษัตริย์ทรงเป็นประมุข สถาบันศาสนา สถาบันพระมหากษัตริย์ ความสัมพันธ์ระหว่างประเทศ การทหารและการข่าวกรองความปลอดภัย และการดำรงชีวิตโดยปกติสุขของประชาชน

๒.๑.๓ ข้อมูลสาธารณะ หมายถึง ข้อมูลที่สามารถเปิดเผยได้หรือข่าวสารสาธารณะที่หน่วยงานจัดทำและครอบครองในรูปแบบและช่องทางดิจิทัล เพื่อให้ประชาชนเข้าถึงได้โดยสะดวก มีส่วนร่วมและตรวจสอบการดำเนินงานของรัฐ และสามารถนำข้อมูลไปพัฒนาบริการและนวัตกรรมที่จะเป็นประโยชน์ต่อประเทศในด้านต่าง ๆ ได้

๒.๑.๔ ข้อมูลความลับทางราชการ หมายถึง ข้อมูลข่าวสารตามมาตรา ๑๔ หรือมาตรา ๑๕ ตามพระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ. ๒๕๔๐ ที่มีคำสั่งไม่ให้เปิดเผยและอยู่ในความครอบครองหรือควบคุมดูแลของสำนักงานซึ่งกำหนดให้มีชั้นความลับตามระเบียบว่าด้วยการรักษาความลับของทางราชการ พ.ศ. ๒๕๔๔ และที่แก้ไขเพิ่มเติม

๒.๑.๕ ข้อมูลที่ใช้ภายในหน่วยงาน หมายถึง ข้อมูลที่ใช้ภายในสำนักงาน และข้อมูลที่เปิดเผยสำหรับผู้มีส่วนได้ส่วนเสียที่จำเป็นต้องใช้ข้อมูลดังกล่าว

/๒.๒ ต้อง ...

๒.๒ ต้องจัดเก็บข้อมูลตามระดับชั้นข้อมูลภาครัฐ โดยแบ่งเป็น ๕ ระดับ ดังนี้

๒.๒.๑ ชั้นเปิดเผย (Open) หมายความถึง ข้อมูลข่าวสารของราชการที่หน่วยงานของรัฐต้องเปิดเผยให้ประชาชนได้รับรู้ รับทราบ หรือตรวจสอบได้โดยไม่จำเป็นต้องร้องขอ

๒.๒.๒ ชั้นเผยแพร่ภายในองค์กร (Private) หมายความถึง ข้อมูลที่สำนักงานไม่ได้เผยแพร่โดยอิสระ โดยทั่วไปจะเกี่ยวข้องกับข้อมูลที่มีลักษณะเป็นส่วนตัว

๒.๒.๓ ชั้นลับ (Confidential) หมายความถึง ข้อมูลข่าวสารลับซึ่งหากเปิดเผยทั้งหมดหรือเพียงบางส่วนจะก่อให้เกิดความเสียหายแก่ประโยชน์แห่งรัฐ

๒.๒.๔ ชั้นลับมาก (Secret) หมายความถึง ข้อมูลข่าวสารลับซึ่งหากเปิดเผยทั้งหมดหรือเพียงบางส่วนจะก่อให้เกิดความเสียหายแก่ประโยชน์แห่งรัฐอย่างร้ายแรง

๒.๒.๕ ชั้นลับที่สุด (Top Secret) หมายความถึง ข้อมูลข่าวสารลับซึ่งหากเปิดเผยทั้งหมดหรือเพียง บางส่วนจะก่อให้เกิดความเสียหายแก่ประโยชน์แห่งรัฐอย่างร้ายแรงที่สุด

ทั้งนี้ ชั้นความลับของข้อมูลทางราชการตามระเบียบว่าด้วยการรักษาความลับของทางราชการ พ.ศ. ๒๕๔๔ มี ๓ ระดับ ได้แก่ ลับที่สุด (Top Secret) ลับมาก (Secret) ลับ (Confidential)

๒.๓ การจัดเก็บแฟ้มข้อมูลลับ ให้ปฏิบัติ ดังนี้

๒.๓.๑ ผู้ที่เป็นเจ้าของแฟ้มข้อมูลลับต้องตรวจสอบความถูกต้องของแฟ้มข้อมูลลับก่อนนำไปใช้งาน

๒.๓.๒ ต้องป้องกันแฟ้มข้อมูลลับที่มีการจัดเก็บไว้ในเครื่องคอมพิวเตอร์ที่ตนเองใช้งานโดยเครื่องคอมพิวเตอร์ต้องมีการตั้งรหัสผ่าน หรือมีระบบรักษาความมั่นคงปลอดภัยตามที่ศูนย์เทคโนโลยีสารสนเทศและเมื่อมีการนำแฟ้มข้อมูลลับไปใช้งานให้ปฏิบัติตามระเบียบว่าด้วยการรักษาความลับของทางราชการ พ.ศ. ๒๕๔๔ และที่แก้ไขเพิ่มเติม อย่างเคร่งครัด

๒.๓.๓ ต้องระมัดระวังการใช้งานแฟ้มข้อมูลลับ การกระจาย หรือแจกจ่ายแฟ้มข้อมูลลับไปยังกลุ่มผู้รับที่มีสิทธิหรือได้รับอนุญาตเท่านั้น

๒.๓.๔ ห้ามแชร์แฟ้มข้อมูลลับบนเครือข่ายสารสนเทศ เพื่อป้องกันบุคคลอื่นหรือผู้ที่ไม่ได้รับอนุญาตอาจเข้าถึงแฟ้มข้อมูลลับได้

๒.๔ การจัดทำสำเนา การแปล การโอน การส่ง การรับ การเก็บรักษา การยืม การทำลาย และการเปิดเผยแฟ้มข้อมูลลับ ให้เป็นไปตามระเบียบว่าด้วยการรักษาความลับของทางราชการ พ.ศ. ๒๕๔๔ และที่แก้ไขเพิ่มเติม

๒.๕ การจัดเก็บข้อมูลส่วนบุคคล ให้เก็บรวบรวมได้เท่าที่จำเป็น ภายใต้อำนาจหน้าที่และวัตถุประสงค์อันชอบตามกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล

๓. การประมวลผลข้อมูลและการใช้ข้อมูล (Data Processing and Use) เพื่อให้การประมวลผลข้อมูลและการใช้ข้อมูลมีประสิทธิภาพ ถูกต้อง ตรงตามวัตถุประสงค์ของการใช้ข้อมูลให้เกิดประโยชน์ รวมถึงวิธีการและแนวทางในการขอข้อมูลจากหน่วยงานต่าง ๆ ให้ดำเนินการ ดังนี้

๓.๑ การนำข้อมูลไปประมวลผลและการใช้ข้อมูลจะต้องได้รับความยินยอมจากเจ้าของข้อมูลก่อน

๓.๒ การนำข้อมูลที่เป็นความลับไปประมวลผลข้อมูล เช่น ข้อมูลส่วนบุคคล ให้เป็นไปตามเงื่อนไขหรือวัตถุประสงค์ในการยินยอมให้ดำเนินการกับข้อมูลส่วนบุคคลนั้น

๓.๓ ต้องมีการบันทึกประวัติการประมวลผลและการใช้ข้อมูล เพื่อให้สามารถตรวจสอบย้อนหลังได้

๓.๔ ผู้ใช้ข้อมูลต้องเป็นผู้รับผิดชอบ หากมีการประมวลผลข้อมูลและการใช้ข้อมูลที่ไม่เป็นไปตามกฎหมายกำหนด

๔. การเปิดเผยข้อมูลและการขอใช้ข้อมูล (Data Disclosure) เป็นการนำข้อมูลที่มีอยู่ในความครอบครองของหน่วยงานมาเผยแพร่ตามช่องทางต่าง ๆ อย่างเหมาะสม เช่น การเปิดเผยข้อมูล (Open Data) การแชร์ข้อมูล (Share) การควบคุมการเข้าถึง (Access Control) การแลกเปลี่ยนข้อมูลระหว่างหน่วยงาน (Exchange) และการกำหนดเงื่อนไขในการนำข้อมูลไปใช้ (Condition) ให้ดำเนินการ ดังนี้

๔.๑ คัดเลือกข้อมูลที่ต้องการเผยแพร่ ให้ปฏิบัติ ดังนี้

๔.๑.๑ เจ้าของข้อมูลและหน่วยงานที่เกี่ยวข้องต้องพิจารณาข้อมูลที่จะเผยแพร่ โดยข้อมูลที่สามารถเผยแพร่ได้จะต้องไม่ขัดต่อกฎหมาย ระเบียบ ข้อบังคับ หรือคำสั่งของสำนักงาน

๔.๑.๒ ต้องเป็นข้อมูลที่สามารถเปิดเผยได้ และไม่ละเมิดข้อมูลส่วนบุคคล เช่น ข้อมูลเชิงสถิติที่ไม่สามารถระบุตัวบุคคลได้ เป็นต้น แต่ในส่วนข้อมูลส่วนบุคคลที่ไม่เปิดเผย เช่น เลขประจำตัวประชาชน เป็นต้น

๔.๒ การพิจารณาชุดข้อมูลที่คัดเลือก ต้องมีรายละเอียดที่อธิบายถึงความเป็นมาของข้อมูล เช่น ชื่อข้อมูล คำอธิบายข้อมูล คำสำคัญ วันที่ทำการเปลี่ยนแปลงข้อมูลล่าสุด ชื่อหน่วยงานเจ้าของข้อมูล และฟิลด์ข้อมูล ทั้งนี้ ต้องตรวจสอบฟิลด์ข้อมูลว่าครบถ้วนและสอดคล้องกับความต้องการของหน่วยงานที่ขอใช้ข้อมูล

๔.๓ การจัดเตรียมข้อมูลให้อยู่ในรูปแบบที่ง่ายต่อการนำไปใช้ ให้ปฏิบัติ ดังนี้

๔.๓.๑ ข้อมูลมีความพร้อมในการส่งต่อหรือเปิดเผยได้ ต้องมีมาตรการรักษาความมั่นคงปลอดภัยที่เหมาะสม เพื่อป้องกันการสูญหายการเข้าถึง การใช้ การเปลี่ยนแปลงและการแก้ไข

๔.๓.๒ การเชื่อมโยงข้อมูลที่มีการจัดเก็บและสามารถเข้าถึงได้เพื่อการตรวจสอบหรือเปิดเผยแก่ผู้ที่เกี่ยวข้อง

๔.๔ การนำชุดข้อมูลขึ้นเผยแพร่ ให้ดำเนินการ ดังนี้

๔.๔.๑ เก็บประวัติ (Log) การเปิดเผย เผยแพร่ข้อมูล เพื่อให้สามารถตรวจสอบได้และเป็นไปตามกฎหมายว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์

๔.๔.๒ มีมาตรการรักษาความมั่นคงปลอดภัยที่เหมาะสม เพื่อป้องกันการสูญหาย การเข้าถึง การใช้ การเปลี่ยนแปลง การแก้ไข

ทั้งนี้ กรณีเป็นข้อมูลส่วนบุคคล การกำหนดเงื่อนไขในการนำข้อมูลไปใช้ (Condition) สำนักงานจะต้องได้รับการยินยอมจากเจ้าของข้อมูลส่วนบุคคล ภายใต้อำนาจหน้าที่และวัตถุประสงค์อันชอบตามกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล

๕. กระบวนการจัดเก็บข้อมูลถาวร (Archive) เป็นการคัดลอกข้อมูลที่มีช่วงอายุเกินช่วงเวลาใช้งานหรือไม่ได้ใช้งานแล้ว เพื่อทำสำเนาสำหรับการเก็บรักษา โดยที่ข้อมูลนั้นไม่มีการลบ ปรับปรุงหรือแก้ไขอีก และสามารถนำกลับมาใช้งานได้ใหม่เมื่อต้องการ การจัดเก็บข้อมูลถาวรให้ปฏิบัติ ดังนี้

๕.๑ กำหนดเครื่องมือและวิธีการที่จะใช้ในการจัดเก็บข้อมูล

๕.๒ กำหนดระยะเวลาในการจัดเก็บข้อมูลแต่ละประเภท

๕.๓ ขอความร่วมมือจากหน่วยงานที่เกี่ยวข้องเพื่อกำหนดระยะเวลาในการจัดเก็บข้อมูลที่เหมาะสมกับข้อมูลแต่ละประเภท

๕.๔ สร้างความรู้ความเข้าใจในการจัดเก็บข้อมูลแก่ผู้ที่เกี่ยวข้อง

๕.๕ ศึกษาข้อมูลที่ต้องการจัดเก็บ โดยเลือกเครื่องมือและกระบวนการที่เป็นมาตรฐานในการจัดเก็บข้อมูลให้อยู่ในสภาพที่พร้อมใช้งานได้ตลอดเวลา

/๖. การ ...

๖. การทำลายข้อมูล (Data Destruction) เป็นการทำลายข้อมูลที่มีการจัดเก็บถาวรเป็นระยะเวลานาน หรือเกินกว่าระยะเวลากำหนด การทำลายข้อมูลให้ปฏิบัติ ดังนี้

๖.๑ ให้กำหนดขั้นตอนและวิธีการทำลายข้อมูล

๖.๒ ขอความร่วมมือจากหน่วยงานที่เกี่ยวข้องเพื่อกำหนดวิธีปฏิบัติการทำลายข้อมูล

๖.๓ หน่วยงานที่ได้รับมอบหมายต้องจัดประชุม/อบรม/ประชาสัมพันธ์ให้ส่วนงานที่เกี่ยวข้องมีความรู้ความเข้าใจวิธีปฏิบัติการทำลายข้อมูล

๖.๔ หน่วยงานที่เกี่ยวข้องต้องกำหนดสิทธิผู้ที่จะดำเนินการทำลายข้อมูล และเก็บประวัติไว้ด้วยทุกครั้ง

๖.๕ หน่วยงานที่เกี่ยวข้องต้องอบรมชี้แจงให้ผู้ปฏิบัติและผู้ที่เกี่ยวข้องมีความรู้ความเข้าใจในการจัดเก็บและทำลายข้อมูล

๖.๖ การทำลายข้อมูลในหนังสือราชการให้เป็นไปตามระเบียบสำนักนายกรัฐมนตรีว่าด้วยงานสารบรรณ พ.ศ. ๒๕๒๖ และที่แก้ไขเพิ่มเติม

ทั้งนี้ กรณีเป็นข้อมูลส่วนบุคคล การทำลายข้อมูลสำนักงานจะต้องมีระบบลบ/ทำลายข้อมูล เมื่อหมดความจำเป็น หรือมีการร้องขอจากเจ้าของข้อมูล หรือที่เจ้าของข้อมูลส่วนบุคคลได้ถอนความยินยอมในการเปิดเผยข้อมูล เว้นแต่ยังมีเหตุทางกฎหมายที่จำเป็นต้องเก็บไว้ ภายใต้อำนาจหน้าที่และวัตถุประสงค์อันชอบตามกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล

หมวด ๒ การแลกเปลี่ยนและเชื่อมโยงข้อมูลระหว่างหน่วยงาน (Data Integration and Exchange)

เพื่อให้การแลกเปลี่ยนข้อมูลระหว่างหน่วยงานมีความถูกต้อง ครบถ้วน ปลอดภัย และมีประสิทธิภาพ โดยมีวิธีและแนวทางการนำข้อมูลไปแลกเปลี่ยนและเชื่อมโยงกับหน่วยงานภายนอกต้องสอดคล้องกับระเบียบ หลักเกณฑ์ และกฎหมายที่กำหนด ให้ดำเนินการ ดังนี้

๑. กำหนดเทคโนโลยีและมาตรฐานทางเทคนิคที่ใช้ในการแลกเปลี่ยนและ/หรือเชื่อมโยงข้อมูล

๒. การแลกเปลี่ยนและ/หรือเชื่อมโยงข้อมูลกับหน่วยงานอื่นจะต้องได้รับอนุญาตจากสำนักงาน และต้องมีการกำหนดความร่วมมือหรือแนวทางการบริหารจัดการข้อมูลร่วมกับหน่วยงานนั้นอย่างชัดเจน เช่น บันทึกข้อตกลง (Memorandum of Understanding: MOU) หรือสัญญารักษาความลับ (Non-Disclosure Agreement: NDA) เป็นต้น

๓. การแลกเปลี่ยนและ/หรือเชื่อมโยงข้อมูลจะต้องมีการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคล โดยให้เป็นไปตามที่กฎหมายกำหนด

๔. เทคโนโลยีและวิธีการทางเทคนิคที่เกี่ยวข้องกับการแลกเปลี่ยนและการเชื่อมโยงข้อมูลต้องเป็นไปตามมาตรฐาน

หมวด ๓ การจัดทำบัญชีข้อมูลของหน่วยงาน (Data Catalog)

๑. เจ้าของข้อมูลหรือผู้ครอบครองข้อมูลมีหน้าที่กำหนดให้มีผู้รับผิดชอบที่เกี่ยวข้องกับข้อมูลของหน่วยงาน

๒. ผู้รับผิดชอบที่เกี่ยวข้องกับข้อมูล มีหน้าที่กำหนดคำนิยามชุดข้อมูล ดังนี้

๒.๑ ความสัมพันธ์ของข้อมูล

๒.๒ ชนิดข้อมูล (Reference/Master Data Definition) แบ่งเป็น

๒.๒.๑ Reference Data หรือ ข้อมูลที่มีลักษณะและโครงสร้างที่เป็นความจริงและถูกต้อง ทำให้ข้อมูลไม่ค่อยเปลี่ยนแปลง ส่งผลให้ข้อมูล Reference Data ถูกเผยแพร่ไปยังแหล่งต่าง ๆ เพื่ออ้างอิงอยู่เสมอ

๒.๒.๒ Master Data หรือ ข้อมูลที่มีโอกาสเปลี่ยนแปลงได้มากกว่า มีรายละเอียดหรือจำนวนฟิลด์ข้อมูลที่มากกว่า Reference Data และใช้เป็นข้อมูลในการดำเนินงานภายในหน่วยงาน

๒.๓ ขอบเขตที่ดำเนินการ

๒.๔ ชุดข้อมูลที่คาดว่าเกี่ยวข้อง

๒.๕ กระบวนงานหลักหรืองานหลักที่ได้รับมอบหมาย และกระบวนงานย่อย

๒.๖ ชุดข้อมูลที่เกี่ยวข้องกับกระบวนงานย่อย แบ่งเป็น ชุดข้อมูลที่มีอยู่แล้ว และชุดข้อมูลที่ต้องการเพิ่มเติม

๒.๗ รูปแบบของการเก็บข้อมูล

๒.๘ ความพร้อมของชุดข้อมูล

๒.๙ การเชื่อมโยงและแลกเปลี่ยนข้อมูลภายในหน่วยงาน

๓. ผู้รับผิดชอบที่เกี่ยวข้องกับข้อมูล มีหน้าที่กำหนด

๓.๑ รายชื่อชุดข้อมูลที่สัมพันธ์กับกระบวนการทำงานตามภารกิจ

๓.๒ คำอธิบายข้อมูล (Metadata) และคำอธิบายข้อมูลของทรัพยากร (Resource Metadata) ที่สอดคล้องตามมาตรฐานที่สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน) (สพร.) กำหนด

๓.๓ พจนานุกรมข้อมูล (Data Dictionary) เช่น ชื่อข้อมูล (Data Namimg) คำอธิบายข้อมูล (Metadata) ชนิดข้อมูล (Data Type) ขนาดของข้อมูล (length of item) รายละเอียดอื่น ๆ (other additional information) เป็นต้น

หมวด ๔ การประเมินคุณภาพข้อมูล (Data Quality Assessment)

หลักเกณฑ์การประเมินคุณภาพข้อมูล (Data Quality Assessment: DQA) มีวัตถุประสงค์เพื่อใช้เป็นกรอบและเครื่องมือสำหรับตรวจสอบคุณภาพข้อมูลเบื้องต้นให้เป็นไปตามกรอบธรรมาภิบาลข้อมูลภาครัฐ โดยจัดทำเกณฑ์ตัวชี้วัดตามมิติคุณภาพข้อมูล ดังนี้

เกณฑ์การประเมินคุณภาพข้อมูล ตามมิติคุณภาพข้อมูล ๕ มิติ ได้แก่ (๑) ความถูกต้อง (๒) ความสอดคล้องกัน (๓) ตรงตามความต้องการของผู้ใช้ (๔) ความเป็นปัจจุบัน และ (๕) ความพร้อมใช้ที่สอดคล้องตามองค์ประกอบในการประเมินคุณภาพข้อมูลตามกรอบธรรมาภิบาลข้อมูลภาครัฐ โดยแต่ละมิติมีรายละเอียดและตัวชี้วัด (indicators) ดังต่อไปนี้

มิติคุณภาพข้อมูล	รายละเอียด	รายการตัวชี้วัด
ความถูกต้อง และสมบูรณ์ (Accuracy and Completeness)	ประเมินเรื่องความถูกต้องแม่นยำ แหล่งข้อมูลที่น่าเชื่อถือ และมีกระบวนการตรวจสอบ	■ มีแหล่งข้อมูลที่น่าเชื่อถือ ■ มีกระบวนการหรือเครื่องมือตรวจสอบจุดผิดพลาดของข้อมูล ■ มีการตรวจสอบความครบถ้วนของข้อมูล ■ มีวิธีเก็บข้อมูลที่มีความเป็นกลาง น่าเชื่อถือ และไม่สร้างข้อมูลที่มีอคติ ■ มีการระบุคำนิยามและลักษณะข้อมูลที่ต้องการ

/มิติ ...

มิติคุณภาพข้อมูล	รายละเอียด	รายการตัวชี้วัด
ความสอดคล้องกัน (Consistency)	ประเมินเรื่องรูปแบบของข้อมูล ความสอดคล้องกัน และมาตรฐานในการจัดทำข้อมูลของหน่วยงาน	■ มีการเก็บข้อมูลภายใต้มาตรฐานข้อมูลเดียวกันหรือมาตรฐานข้อมูลที่สอดคล้องกันทำให้สามารถใช้ประโยชน์ข้อมูลร่วมกันได้ ■ มีการตรวจสอบรูปแบบข้อมูลภายในชุดข้อมูลเดียวกัน ■ ข้อมูลมีความเชื่อมโยงและไม่ขัดแย้งกัน ■ มีการใช้กฎ วิธีการตรวจวัดที่สอดคล้องกันทั้งหน่วยงานรวมถึงหน่วยงานภายนอก ■ มีการกำหนดบทบาทและผู้รับผิดชอบข้อมูล
ตรงตามความต้องการของผู้ใช้ (Relevancy)	ประเมินว่า เป็นข้อมูลที่ผู้ใช้ต้องการ หรือเป็นข้อมูลที่จำเป็นต้องทราบ มีความละเอียดเพียงพอต่อการนำไปใช้งาน	■ ข้อมูลตรงตามความต้องการและวัตถุประสงค์ของการใช้งาน ■ มีผลประเมินความพึงพอใจของผู้ใช้ ■ และมีการปรับปรุงคุณภาพให้ตรงตามความต้องการของผู้ใช้
ความเป็นปัจจุบัน (Timeliness)	ประเมินเรื่องการเผยแพร่ข้อมูล การปรับปรุงข้อมูลและแผนเรื่องระยะเวลา	■ ข้อมูลมีการเผยแพร่ ส่งต่อตรงเวลา ■ ข้อมูลมีความเป็นปัจจุบัน ■ ข้อมูลมีการเผยแพร่ในเวลาที่เหมาะสม ■ มีการจัดทำปฏิทินเผยแพร่ข้อมูล
ความพร้อมใช้ (Availability)	ประเมินความพร้อมใช้ของข้อมูล รวมไปถึงช่องทางในการขอหรือใช้ข้อมูล	■ ข้อมูลถูกจัดในรูปแบบที่พร้อมนำไปใช้งานและเหมาะสมกับผู้ใช้งาน ■ มีการเผยแพร่ข้อมูลที่เหมาะสมและสามารถเข้าถึงได้ โดยผู้ใช้สามารถเข้าถึงข้อมูลได้สะดวกตามสิทธิที่เหมาะสม ■ ข้อมูลสามารถอ่านด้วยโปรแกรมคอมพิวเตอร์ได้ ■ มีคำอธิบายข้อมูลที่ชัดเจน ■ มีคำอธิบายขั้นตอนการขอข้อมูลที่ไม่เผยแพร่เป็นสาธารณะสำหรับหน่วยงานภายนอก

เครื่องมือการประเมินคุณภาพข้อมูล ในการประเมินคุณภาพข้อมูล เจ้าของข้อมูลหรือผู้ครอบครองข้อมูลสามารถใช้เครื่องมือการประเมินคุณภาพข้อมูล เพื่อตรวจสอบและควบคุมการบริหารจัดการข้อมูล เพื่อให้ได้ข้อมูลที่มีคุณภาพ น่าเชื่อถือ รวมทั้งสามารถนำไปใช้ประโยชน์เพื่อเพิ่มประสิทธิภาพในการทำงาน เพิ่มคุณค่าในการให้บริการภาครัฐ โดยเครื่องมือการประเมินคุณภาพข้อมูล มี ๓ ประเภท คือ

๑. แบบตรวจประเมินคุณภาพ (DQA Checklist) เพื่อประเมินกระบวนการเตรียมข้อมูลให้มีคุณภาพ ตามมิติคุณภาพข้อมูล ๕ มิติ

/๒. แบบประเมิน ...

๒. แบบประเมินคุณภาพข้อมูลด้วยตนเอง (DQA Self-Assessment) เพื่อประเมินชุดข้อมูลตามมิติคุณภาพข้อมูล ๕ มิติ เพื่อให้ทราบว่าข้อมูลภายในหน่วยงานมีคุณภาพมากน้อยเพียงใด และควรปรับปรุงหรือพัฒนาในมิติใด

๓. แบบตรวจประเมินการควบคุมและติดตามคุณภาพข้อมูล (Data Quality Monitoring and Control Checklist) เพื่อตรวจสอบหลักฐานในการสนับสนุนกระบวนการเผยแพร่ข้อมูลที่มีคุณภาพตั้งแต่การจัดเตรียมข้อมูล การเผยแพร่ข้อมูล และการรายงานผลข้อมูล เพื่อกำหนดเป็นมาตรฐานในการดำเนินงานในหน่วยงาน

หมวด ๕ การจัดระดับชั้นข้อมูล

เกณฑ์พิจารณากำหนดระดับชั้นข้อมูลสำหรับทุกชุดข้อมูล (Dataset) ที่แลกเปลี่ยนกันได้ในรูปแบบอิเล็กทรอนิกส์ทุกประเภท ซึ่งรวมถึงข้อมูลลับในรูปแบบอิเล็กทรอนิกส์ของหน่วยงานภาครัฐ โดยจะไม่ครอบคลุมเอกสารที่เป็นกระดาษทุกประเภท เพื่อเป็นเครื่องมือประกอบการใช้ดุลพินิจของผู้มีอำนาจในการตัดสินใจกำหนดระดับชั้นข้อมูล สามารถกำหนดการเข้าถึงและใช้งานข้อมูลและกำกับดูแลข้อมูลที่มีความอ่อนไหวหรือข้อมูลที่มีระดับชั้นความลับอย่างเหมาะสมเพื่อรักษาความเป็นส่วนตัวและความปลอดภัยของข้อมูล รวมทั้งกำหนดนโยบายการแบ่งปันข้อมูลระหว่างหน่วยงานภาครัฐโดยไม่ขัดต่อข้อกฎหมายที่เกี่ยวข้อง

การจัดระดับชั้นข้อมูลภาครัฐเจ้าของข้อมูลหรือผู้ครอบครองข้อมูลสามารถจัดระดับตามผลกระทบที่จะเกิดขึ้นตามมาตรฐานและข้อกฎหมายที่เกี่ยวข้อง เพื่อให้สามารถจัดการข้อมูลในกระบวนงานที่เกี่ยวข้องกับภารกิจได้อย่างมีประสิทธิภาพ ซึ่งระดับชั้นข้อมูลสามารถแบ่งได้ ๕ ระดับ ได้แก่

๑) ชั้นเปิดเผย (Open) เป็นข้อมูลข่าวสารของราชการที่หน่วยงานของรัฐต้องเปิดเผยให้ประชาชนได้รับรู้ รับทราบ หรือตรวจสอบได้โดยไม่จำเป็นต้องร้องขอ เช่น กฎ มติคณะรัฐมนตรี ข้อบังคับ รายงานผลการศึกษาทางวิชาการ และข้อมูลเปิดภาครัฐ ฯลฯ

๒) ชั้นเผยแพร่ภายในองค์กร (Private) เปิดเผยเมื่อได้รับอนุญาต เป็นข้อมูลที่สำนักงานไม่ได้เผยแพร่โดยอิสระ โดยทั่วไปจะเกี่ยวข้องกับข้อมูลที่มีลักษณะเป็นส่วนตัว ไม่ว่าจะเป็นข้อมูลบุคคลหรือองค์กร และแม้ว่าการสูญเสียข้อมูลหรือการเปิดเผยข้อมูลอาจไม่ส่งผลให้เกิดผลกระทบที่สำคัญ แต่ก็ไม่พึงประสงค์ที่ให้เปิดเผยโดยไม่ได้รับอนุญาต เช่น ข้อมูลระเบียน ข้อมูลพนักงาน เอกสารประกอบการปฏิบัติงานและวิธีปฏิบัติภายในหน่วยงาน ฯลฯ

๓) ชั้นลับ (Confidential) เปิดเผยเมื่อได้รับอนุญาต เป็นข้อมูลที่จัดระดับชั้นลับ หรือมีความอ่อนไหว ซึ่งหากมีการเปิดเผยต่อบุคคล/องค์กรที่ไม่ได้รับอนุญาต จะส่งผลให้เกิดความอับอายอย่างมากต่อบุคคล/องค์กร และอาจเป็นผลทางกฎหมาย หรือจะก่อให้เกิดความเสียหายแก่ ผลประโยชน์แห่งรัฐ เช่น ข้อมูลการฟ้องคดี และความเห็นภายในหน่วยงานที่ยังไม่ได้ข้อยุติ ฯลฯ

๔) ชั้นลับมาก (Secret) เปิดเผยเมื่อได้รับอนุญาต เป็นข้อมูลที่จัดระดับชั้นลับมาก หรือมีความอ่อนไหวปานกลาง ซึ่งหากสูญหายหรือเปิดเผยอย่างไม่ถูกต้องเหมาะสม จะก่อให้เกิดความสูญเสีย/ผลกระทบร้ายแรง อาจทำให้เสียชื่อเสียงและการสูญเสียทางการเงิน/ทรัพย์สิน ต่อความมั่นคงและผลประโยชน์แห่งรัฐอย่างร้ายแรง หรือที่มีนัยสำคัญ (Importance) เช่น รายงานการแพทย์ ข้อมูลความสัมพันธ์ระหว่างประเทศ และนโยบายสำคัญที่ใช้ปฏิบัติต่อรัฐต่างประเทศ ฯลฯ

๕) ชั้นลับที่สุด (Top Secret) เปิดเผยไม่ได้ เป็นข้อมูลที่จัดระดับชั้นลับที่สุด หรือมีความอ่อนไหวมาก ซึ่งหากสูญหายหรือเปิดเผยอย่างไม่ถูกต้องเหมาะสม จะก่อให้เกิดความสูญเสีย/ผลกระทบร้ายแรงที่สุด อาจทำให้ชื่อเสียง และการสูญเสียทางการเงิน/ทรัพย์สิน ต่อความมั่นคงและผลประโยชน์แห่งรัฐอย่างร้ายแรง หรือที่สำคัญยิ่งยวด (Vital) ในกรณีข้อมูลที่อยู่ในชั้น “ลับที่สุด” จะถูกจำกัดการใช้ ไม่เปิดเผยและไม่สามารถนำเข้าในระบบสารสนเทศได้ ต้องดำเนินการในรูปแบบเอกสาร (Hard Copy) เท่านั้น เช่น ข้อมูลกำลังรบ ข้อมูลด้านการข่าวกรองยุทธศาสตร์ ข้อมูลความมั่นคงเชิงนโยบาย

/หมวด ๖ ...

หมวด ๖ การบริหารจัดการข้อมูล

การบริหารจัดการข้อมูลแบ่งตามวงจรชีวิตข้อมูล ได้แก่ ๑. การสร้างข้อมูล ๒. การจัดเก็บข้อมูล ๓. การประมวลผลข้อมูลและการใช้ข้อมูล ๔. การเปิดเผยข้อมูล ๕. การทำลายข้อมูล ๖. การเชื่อมโยงและการแลกเปลี่ยนข้อมูล ในแต่ละข้อจะระบุ ผู้รับผิดชอบงาน ข้อปฏิบัติ และเอกสารประกอบการบริหารจัดการข้อมูล

๑. การสร้างข้อมูล ในการสร้างข้อมูลผู้ที่เกี่ยวข้องต้องสร้างข้อมูลให้มีคุณภาพ มีความมั่นคงปลอดภัย และเป็นประโยชน์ต่อผู้ใช้ข้อมูล โดยมีผู้รับผิดชอบงาน ดังนี้

- ผู้สร้างข้อมูล (Data Creators)
- ทีมบริหารจัดการข้อมูล (Data Management Team)
- เจ้าของข้อมูล (Data Owners)
- บริกรข้อมูล (Data Stewards)
- ผู้ดูแลระบบสารสนเทศ (System Administrators)

ข้อปฏิบัติ

๑. เจ้าของข้อมูล (ไม่ว่า เจ้าของข้อมูล จะอยู่ภายใน สำนัก/ศูนย์/กลุ่ม เดียว หรือ มากกว่าหลาย สำนัก/ศูนย์/กลุ่ม ต้องมีการกำหนดชัดเจน ถึงอำนาจหน้าที่และขั้นตอนการทำงานร่วมกัน)

๑.๑ กำหนดผู้มีสิทธิในการสร้างข้อมูล และจะต้องทบทวนสิทธินั้น อย่างน้อยปีละ ๑ ครั้ง หรือเมื่อมีการเปลี่ยนแปลงที่สำคัญ เช่น การลาออก เปลี่ยนตำแหน่ง โอนย้าย สิ้นสุดการจ้าง การปรับโครงสร้าง หรือเมื่อมีการปรับปรุงระบบสารสนเทศ เป็นต้น

๑.๒ กำหนดหมวดหมู่และชั้นความลับของข้อมูล

๒. ผู้ดูแลระบบสารสนเทศจะต้องกำหนดสิทธิในการสร้างข้อมูลในระบบให้แก่ผู้สร้างข้อมูลตามที่เจ้าของข้อมูลกำหนด

๓. เจ้าของข้อมูล บริกรข้อมูล และทีมบริหารจัดการข้อมูล ร่วมจัดทำคำอธิบาย ชุดข้อมูลดิจิทัลหรือเมทาดาตา (Metadata) เมื่อมีการสร้างชุดข้อมูล (Datasets) ตามมาตรฐานขั้นต่ำคำอธิบายชุดข้อมูลดิจิทัลที่สำนักงานพัฒนารัฐบาลดิจิทัล (สพร.) กำหนด และกำหนดให้ทำการประเมินคุณค่าของชุดข้อมูลดิจิทัลตามแบบฟอร์มประเมินคุณค่าชุดข้อมูลที่ สพร. หรือหน่วยงานกำหนด เพื่อสนับสนุนการคัดเลือกเป็นชุดข้อมูลคุณค่าสูง (High Value Dataset) และเผยแพร่เป็นข้อมูลเปิดของหน่วยงานต่อสาธารณะตามกฎหมายว่าด้วยข้อมูลข่าวสารของราชการในรูปแบบข้อมูลดิจิทัล

๔. ห้ามมิให้ผู้สร้างข้อมูลนำข้อมูลที่ขัดต่อกฎหมายว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์เข้าสู่ระบบคอมพิวเตอร์ ซึ่งมีลักษณะดังต่อไปนี้

- ข้อมูลที่บิดเบือน หรือข้อมูลปลอมไม่ว่าทั้งหมดหรือบางส่วน
- ข้อมูลอันเป็นเท็จที่น่าจะเกิดความเสียหายต่อการรักษาความมั่นคงปลอดภัย ความปลอดภัยสาธารณะ ความมั่นคงทางเศรษฐกิจ หรือ โครงสร้างพื้นฐาน หรือ ก่อให้เกิดความตื่นตระหนก
- ข้อมูลอันเป็นความผิดเกี่ยวกับความมั่นคง หรือ ความผิดเกี่ยวกับการก่อการร้าย
- ข้อมูลที่มีลักษณะอันลามก และคนทั่วไปอาจเข้าถึงได้
- ข้อมูลที่ปรากฏภาพของผู้อื่น และเป็นภาพที่สร้างขึ้น ตัดต่อ เติม หรือดัดแปลงด้วยวิธีการทางอิเล็กทรอนิกส์ ทำให้ผู้อื่นเสียชื่อเสียง ถูกดูหมิ่นถูกเกลียดชัง หรือ ได้รับความอับอาย

๕. ห้ามมิให้ผู้สร้างข้อมูล ทำการสร้าง/ทำซ้ำต่อข้อมูลที่ขัดต่อกฎหมายว่าด้วยลิขสิทธิ์หรือทรัพย์สินทางปัญญาของผู้อื่น เว้นแต่จะเป็นไปตามอำนาจที่กฎหมายรับรอง

/๖. กำหนด ...

๖. กำหนดให้ผู้สร้างข้อมูลสร้างข้อมูลที่มาจากแหล่งข้อมูลที่เชื่อถือได้เท่านั้น

๗. กำหนดให้เจ้าของข้อมูลตรวจสอบความถูกต้องของข้อมูลที่ถูกสร้างขึ้น

๘. ข้อปฏิบัติอื่น ๆ ตามที่หน่วยงานกำหนดเพิ่มเติม

๒. การจัดเก็บข้อมูล ในการจัดเก็บข้อมูลผู้ที่เกี่ยวข้องต้องจัดเก็บข้อมูลให้มีคุณภาพ เข้าถึง และใช้งานได้อย่างมั่นคงปลอดภัย โดยมีผู้รับผิดชอบงาน ดังนี้

- เจ้าของข้อมูล (Data Owners)
- ผู้ดูแลระบบสารสนเทศ (System Administrators)
- ผู้สร้างข้อมูล (Data Creators)
- บริกรข้อมูล (Data Stewards)
- ผู้ใช้ข้อมูล (Data Users)
- ทีมบริหารจัดการข้อมูล (Data Management Team)

ข้อปฏิบัติ

๑. กำหนดให้เจ้าของข้อมูลจะต้องกำหนดระยะเวลาในการจัดเก็บข้อมูลที่ชัดเจน

๒. กำหนดให้ทีมบริหารจัดการข้อมูล และผู้ดูแลระบบสารสนเทศทำการย้ายข้อมูลที่มีการจัดเก็บเกินระยะเวลาที่กำหนดแล้วเพื่อจัดเก็บเป็นข้อมูลถาวร

๓. กำหนดให้การจัดเก็บชุดข้อมูลจะต้องมีคำอธิบายชุดข้อมูลดิจิทัลหรือเมทาดาตา หากไม่มีหรือ ไม่ครบถ้วน ทีมบริหารจัดการข้อมูลจะต้องแจ้งผู้รับผิดชอบ ได้แก่ เจ้าของข้อมูล บริกรข้อมูลด้านเทคนิค และบริกรข้อมูลด้านธุรกิจ โดยทีมบริหารจัดการข้อมูลร่วมกันจัดทำและปรับปรุงให้เป็นปัจจุบัน

๔. ผู้มีส่วนได้ส่วนเสียเกี่ยวข้องกับข้อมูล ทั้งเจ้าของข้อมูล ผู้สร้างข้อมูล ผู้ใช้ข้อมูล และทีมบริหารจัดการข้อมูล จะต้องจัดเก็บข้อมูลตามการจัดชั้นความลับของหน่วยงาน โดยทำการเข้ารหัสข้อมูลเพื่อป้องกันการเข้าถึงหรือแก้ไขข้อมูลโดยไม่ได้รับอนุญาต ทั้งนี้การเข้ารหัสข้อมูลให้ปฏิบัติตามวิธีการเข้ารหัสข้อมูลแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงาน

๔.๑ ในกรณีที่ในตารางฐานข้อมูลเดียวกันมีฟิลด์ข้อมูลที่มีชั้นความลับและไม่มีชั้นความลับอยู่ร่วมกันให้ทำการเข้ารหัสข้อมูลเฉพาะฟิลด์ข้อมูลที่มีชั้นความลับเท่านั้น

๔.๒ ในกรณีข้อมูลที่จัดเก็บในรูปแบบเอกสาร ให้มีการจัดเก็บ ดังนี้

- เก็บในสถานที่เหมาะสม สามารถปิดล็อกได้เมื่อไม่ใช้งาน
- เก็บแยกออกจากอุปกรณ์ประมวลผลต่าง ๆ เช่น เครื่องพิมพ์ เครื่องถ่ายเอกสาร เป็นต้น โดยทันที เพื่อเป็นการป้องกันไม่ให้ผู้ไม่มีสิทธิในการเข้าถึงข้อมูล เข้าถึงข้อมูลได้

๕. กำหนดให้มีวิธีปฏิบัติการกู้คืนข้อมูลที่จัดเก็บถาวร สำหรับข้อมูลที่มีความสำคัญมากต่อการดำเนินงานของหน่วยงาน เพื่อสอบทานความถูกต้อง ครบถ้วน ความพร้อมใช้งาน คุณภาพข้อมูล

๖. ในการจัดเก็บข้อมูลส่วนบุคคลให้เก็บรวบรวมได้เท่าที่จำเป็น ภายใต้อำนาจหน้าที่และวัตถุประสงค์อันชอบด้วยกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล และไม่เก็บรวบรวมข้อมูลส่วนบุคคล เว้นแต่ได้รับการยินยอมจากเจ้าของข้อมูลส่วนบุคคล หรือพระราชบัญญัติว่าด้วยการคุ้มครองข้อมูลส่วนบุคคลหรือกฎหมายอื่นบัญญัติให้กระทำได้

๗. กำหนดให้มีการยกเลิกการจัดเก็บข้อมูลส่วนบุคคลกรณีเจ้าของข้อมูลส่วนบุคคลถอนความยินยอมตามที่กฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคลกำหนด

/๘. ในกรณี ...

๘. ในกรณีที่มีการประชุมหรือธุรกรรมออนไลน์ กำหนดให้มีการจัดเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ไว้ไม่น้อยกว่า ๙๐ วัน นับแต่วันที่ข้อมูลเข้าสู่ระบบคอมพิวเตอร์ โดยจัดเก็บรักษาข้อมูลของผู้ใช้บริการเท่าที่จำเป็นเพื่อให้สามารถระบุตัวผู้ใช้บริการนับแต่เริ่มใช้บริการให้สอดคล้องตามกฎหมายว่าด้วยการกระทำความผิดทางคอมพิวเตอร์และในการจัดเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ให้สอดคล้องตามกฎหมายว่าด้วยการกระทำความผิดทางคอมพิวเตอร์ ผู้ให้บริการจะต้องใช้วิธีการที่มั่นคงปลอดภัยอย่างน้อย ดังนี้

- เก็บลงในสื่อที่รักษาความครบถ้วนถูกต้องแท้จริง (Integrity) และระบุตัวตน (Identification) ที่เข้าถึงสื่อได้

- มีการรักษาความลับของข้อมูล และกำหนดชั้นความลับในการเข้าถึงและจัดเก็บข้อมูล เพื่อรักษาความน่าเชื่อถือของข้อมูล และไม่อนุญาตให้ผู้ดูแลระบบแก้ไขข้อมูลที่จัดเก็บไว้ได้

- การจัดเก็บข้อมูลระบุรายละเอียดผู้ใช้บริการเป็นรายบุคคลได้ (Identification and Authentication) เช่น Proxy Server NAT และอื่น ๆ

๙. กำหนดให้มีมาตรการรักษาความปลอดภัยในการจัดเก็บข้อมูล รวมทั้งกรณีที่มีการเคลื่อนย้ายอุปกรณ์ที่จัดเก็บข้อมูล เพื่อป้องกันมิให้มีการเข้าถึงโดยมิได้รับอนุญาต หรือลักลอบนำข้อมูลไปใช้ที่ก่อให้เกิดความเสียหายต่อหน่วยงาน

๑๐. กำหนดมาตรการรักษาความปลอดภัยของข้อมูลที่จัดเก็บถาวร เพื่อป้องกันข้อมูลไม่ให้มีการลบ ปรับปรุง แก้ไขได้ รวมทั้งป้องกันมิให้ข้อมูลที่จัดเก็บถาวรรั่วไหลไปยังบุคคลที่ไม่ได้รับอนุญาต

๑๑. กำหนดให้มีมาตรการรักษาความปลอดภัยของการถ่ายโอนข้อมูลกับหน่วยงานภายนอกที่ผ่านช่องทางการสื่อสารทุกชนิด โดยต้องสอดคล้องตามนโยบายความมั่นคงปลอดภัยสารสนเทศ

๑๒. ห้ามมิให้จัดเก็บข้อมูลส่วนตัวหรือข้อมูลที่ไม่เกี่ยวข้องกับการดำเนินงานของหน่วยงาน สำหรับการจัดเก็บข้อมูลถาวรบนเครื่องแม่ข่ายที่หน่วยงานจัดสรรไว้

๑๓. กำหนดให้มีการทบทวนเกี่ยวกับช่วงระยะเวลาการจัดเก็บข้อมูล มาตรการ และวิธีปฏิบัติที่เกี่ยวข้องกับการจัดเก็บข้อมูลถาวร อย่างน้อยปีละ ๑ ครั้ง

๑๔. ข้อปฏิบัติอื่น ๆ ตามที่หน่วยงานกำหนดเพิ่มเติม

๓. การประมวลผลข้อมูลและการใช้ข้อมูล ในการประมวลผลข้อมูลและการใช้ข้อมูลผู้ที่เกี่ยวข้องต้องประมวลผลและใช้ข้อมูลให้มีประสิทธิภาพ ถูกต้อง ตรงตามวัตถุประสงค์ เพื่อให้เกิดประโยชน์สูงสุด โดยมีผู้รับผิดชอบงาน ดังนี้

- เจ้าของข้อมูล (Data Owners)
- ผู้ใช้ข้อมูล (Data Users)
- ผู้ดูแลระบบสารสนเทศ (System Administrators)

ข้อปฏิบัติ

๑. เจ้าของข้อมูลจะต้องกำหนดผู้มีสิทธิเข้าถึงเพื่อประมวลผลและใช้ข้อมูลตามชั้นความลับ ดังนี้

- ข้อมูลเปิดเผยได้ ไม่กำหนดสิทธิการเข้าถึงเพื่อประมวลผลและใช้งานข้อมูล
- ข้อมูลที่มีชั้นความลับ กำหนดให้ผู้ใช้งานที่ได้รับสิทธิเข้าถึงและใช้ข้อมูลตามอำนาจหน้าที่เท่านั้น
- ข้อมูลใช้ภายใน กำหนดให้บุคลากรของหน่วยงานเท่านั้นที่มีสิทธิเข้าถึงเพื่อประมวลผลและใช้งานข้อมูลได้

/๒. ผู้ ...

๒. ผู้ดูแลระบบสารสนเทศจะต้องกำหนดสิทธิในการเข้าถึงข้อมูลในระบบเพื่อประมวลผลและใช้ข้อมูลของผู้ใช้งานตามที่เจ้าของข้อมูลกำหนด

๓. เจ้าของข้อมูลจะต้องทบทวนสิทธิการเข้าถึงเพื่อประมวลผลและใช้ข้อมูลของผู้ใช้งานอย่างน้อยปีละ ๑ ครั้ง หรือเมื่อมีการเปลี่ยนแปลงที่สำคัญ เช่น การลาออก เปลี่ยนตำแหน่ง โอนย้าย สิ้นสุดการจ้าง การปรับโครงสร้าง หรือเมื่อมีการปรับปรุงระบบสารสนเทศ เป็นต้น

๔. ผู้ที่มีสิทธิเข้าใช้งานข้อมูลที่มีชั้นความลับตามที่กำหนดโดยเจ้าของข้อมูลจะต้องใช้ข้อมูลอย่างระมัดระวัง โดยคำนึงถึงความปลอดภัยและต้องไม่ใช้งานข้อมูลที่มีชั้นความลับในพื้นที่สาธารณะ

๕. ผู้ใช้ข้อมูลจะประมวลผลข้อมูลหรือใช้ข้อมูลส่วนบุคคลเท่าที่จำเป็นภายใต้อำนาจหน้าที่และวัตถุประสงค์อันชอบด้วยกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล หรือตามคำสั่งที่ได้รับจากหน่วยงานเท่านั้น เว้นแต่คำสั่งนั้นขัดต่อกฎหมายหรือบทบัญญัติในการคุ้มครองข้อมูลส่วนบุคคล

๖. หน่วยงานต้องยกเลิกการประมวลผลข้อมูลหรือการใช้ข้อมูลส่วนบุคคล กรณีที่เจ้าของข้อมูลส่วนบุคคลถอนความยินยอมตามที่กฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคลกำหนด

๗. ผู้ใช้ข้อมูลจะต้องไม่ใช้ข้อมูลในเครือข่ายของหน่วยงานเพื่อประโยชน์ในเชิงธุรกิจเป็นการส่วนตัวหรือเพื่อเข้าสู่เว็บไซต์ที่ไม่เหมาะสมหรือใช้ข้อมูลอันก่อให้เกิดความเสียหายต่อหน่วยงาน

๘. ข้อปฏิบัติอื่น ๆ ตามที่หน่วยงานกำหนดเพิ่มเติม

๔. การเปิดเผยข้อมูล ในการเปิดเผยข้อมูลผู้ที่เกี่ยวข้องต้องเปิดเผยข้อมูลต่อสาธารณะโดยอิงจากกฎหมาย กฎเกณฑ์ และแนวปฏิบัติที่เกี่ยวข้อง ทั้งนี้ข้อมูลที่เปิดเผยควรเป็นประโยชน์ สามารถนำไปประมวลผลและใช้ต่อยอดในการพัฒนาในรูปแบบต่าง ๆ ได้ โดยมีผู้รับผิดชอบงาน ดังนี้

- เจ้าของข้อมูล (Data Owners)
- ผู้ใช้ข้อมูล (Data Users)
- บริกรข้อมูล (Data Stewards)
- ทีมบริหารจัดการข้อมูล (Data Management Team)

ข้อปฏิบัติ

๑. เจ้าของข้อมูลจะต้องเปิดเผยข้อมูลในความรับผิดชอบต่อสาธารณะตามกฎหมายว่าด้วยข้อมูลข่าวสารของราชการ และมาตรฐานและหลักเกณฑ์การเปิดเผยข้อมูลเปิดภาครัฐในรูปแบบข้อมูลดิจิทัลต่อสาธารณะ

๒. เจ้าของข้อมูลทำการเปิดเผยข้อมูลในความรับผิดชอบในรูปแบบที่ข้อมูลเปิดของหน่วยงานโดยดำเนินการ ดังนี้

- กำหนดลักษณะของข้อมูลที่เผยแพร่กำหนดให้อยู่ในรูปแบบที่เครื่องสามารถประมวลผลได้
- กำหนดให้มีคำอธิบายข้อมูลหรือเมทาดาตาสำหรับข้อมูลที่ต้องเปิดเผย
- ข้อมูลที่เผยแพร่จะต้องมีการบันทึกเวลา (Timestamps) ที่ช่วยให้ผู้ใช้งานสามารถระบุได้ว่าข้อมูลนั้นเป็นปัจจุบัน
- ข้อมูลที่เผยแพร่ต้องมาจากแหล่งที่เก็บข้อมูลโดยตรง ด้วยระดับความละเอียดสูงโดยไม่มีการปรับแต่งหรือเป็นข้อมูลรูปแบบสรุป (Summary data)
- ชุดข้อมูลและรายการชุดข้อมูลที่เผยแพร่จะต้องมีการจัดรูปแบบที่กำหนดเป็นมาตรฐาน และกำหนดภายใต้หมวดหมู่เดียวกัน เพื่อให้ผู้ใช้ข้อมูลสามารถค้นหาและเข้าถึงข้อมูลได้ง่าย

/๓. กำหนด ...

๓. กำหนดให้เงื่อนไขและข้อกำหนดของข้อมูลที่นำมาเปิดเผยภายในเครือข่ายของหน่วยงาน ข้อมูลที่เผยแพร่ต้องไม่ขัดต่อกฎหมายว่าด้วยทรัพย์สินทางปัญญา เว้นแต่การเปิดเผยข้อมูลจะเป็นไปตามอำนาจที่กฎหมายรับรอง

๔. สนับสนุนการจัดทำบัญชีข้อมูลหน่วยงานและการลงทะเบียนบัญชีข้อมูลภาครัฐ โดยบริหารจัดการข้อมูลสำคัญ จัดทำบัญชีข้อมูลของหน่วยงาน และทำการลงทะเบียนบัญชีข้อมูลของหน่วยงานและ ชุดข้อมูลสำคัญ เข้าสู่ระบบบัญชีข้อมูลภาครัฐ (Government Data Catalog หรือ GD Catalog) เพื่อการเปิดเผยข้อมูลภาครัฐที่เป็นระบบ และมีเอกภาพ สามารถสืบค้นชุดข้อมูล คำอธิบายชุดข้อมูล รวมไปถึงแหล่งต้นทางของชุดข้อมูลภาครัฐที่สำคัญ สนับสนุนการใช้ประโยชน์ข้อมูลภาครัฐร่วมกัน

๕. สนับสนุนการเผยแพร่ข้อมูลผ่านช่องทางที่ง่ายต่อการเข้าถึงข้อมูล และสนับสนุนการเปิดเผยข้อมูลในรูปแบบดิจิทัลต่อสาธารณะที่ศูนย์กลางข้อมูลเปิดภาครัฐ (Government Open Data) ผ่านเว็บไซต์ data.go.th โดย

- กำหนดให้มีมาตรการรักษาความมั่นคงปลอดภัยในการเปิดเผยข้อมูลที่กำหนดลำดับชั้นข้อมูลตั้งแต่ลับขึ้นไปอย่างเพียงพอและมีประสิทธิภาพ
- มีการตรวจสอบข้อมูลที่เผยแพร่จากหน่วยงานทั้งภายในและภายนอกหน่วยงาน เพื่อให้มั่นใจว่าหน่วยงานได้มีข้อมูลที่เผยแพร่ที่มีคุณค่า
- การเผยแพร่ข้อมูล ต้องมีการตรวจสอบรูปแบบข้อมูลที่เผยแพร่ให้สอดคล้องกับมาตรฐานที่หน่วยงานกำหนด
- หากการเปิดเผยนั้นเป็นการเปิดเผยบนช่องทางที่ดูแลรับผิดชอบโดยหน่วยงานอื่นที่ให้ปฏิบัติตามเอกสารคู่มือการนำข้อมูลขึ้นเผยแพร่ของหน่วยงานนั้น
- หากการเปิดเผยข้อมูลไม่ครบถ้วน หรือไม่เป็นปัจจุบัน ให้แจ้งเจ้าของข้อมูล บริกรข้อมูล และทีมบริหารจัดการข้อมูลทำการจัดทำ/ปรับปรุงให้เป็นปัจจุบัน

๖. กำหนดให้เปิดเผยข้อมูลส่วนบุคคลตามข้อกำหนดของพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ หรือตามคำสั่งที่ได้รับจากหน่วยงานเท่านั้น เว้นแต่คำสั่งนั้นขัดต่อกฎหมายหรือบทบัญญัติในกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล

๗. เจ้าของข้อมูลห้ามเปิดเผยข้อมูลความมั่นคงและข้อมูลความลับทางราชการที่อยู่ในความครอบครองของหน่วยงานรวมทั้งห้ามเปิดเผยข้อมูลที่เป็นการกระทำความผิดตามกฎหมาย นโยบายและแนวปฏิบัติอันทำให้เกิดความเสียหายต่อหน่วยงาน

๘. กำหนดให้เจ้าของข้อมูลคัดเลือกข้อมูลที่จะเปิดเผยในรูปแบบข้อมูลเปิดจากลำดับชั้นความสำคัญของชุดข้อมูลที่มีคุณค่าสูง (High Value Dataset)

๙. กำหนดให้เจ้าของข้อมูลต้องกำหนดรอบระยะเวลาในการตรวจสอบและปรับปรุงข้อมูลที่เปิดเผยเพื่อให้ข้อมูลถูกต้อง และเป็นปัจจุบัน

๑๐. ข้อปฏิบัติอื่นๆ ตามที่หน่วยงานกำหนดเพิ่มเติม

๕. การทำลายข้อมูล ในการทำลายข้อมูลผู้ที่เกี่ยวข้องต้องปฏิบัติตามแนวปฏิบัติธรรมาภิบาลข้อมูลของสำนักงาน หมวด ๑ วงจรชีวิตข้อมูล (Data Life Cycle) ข้อ ๖ การทำลายข้อมูล (Data Destruction) เพื่อเป็นการรักษาความมั่นคงปลอดภัยของข้อมูล โดยมีผู้รับผิดชอบงาน ดังนี้

- เจ้าของข้อมูล (Data Owners)
- ผู้ทำลายข้อมูล (Data Disposer)
- ผู้ดูแลระบบสารสนเทศ (Systems Administrators)

/ข้อปฏิบัติ ...

ข้อปฏิบัติ

๑. เจ้าของข้อมูลเป็นผู้กำหนดผู้มีสิทธิในการทำลายข้อมูล และจะต้องทบทวนสิทธินั้นอย่างน้อยปีละ ๑ ครั้ง หรือเมื่อมีการเปลี่ยนแปลงที่สำคัญ เช่น การลาออก เปลี่ยนตำแหน่ง โอนย้าย สิ้นสุดการจ้าง การปรับโครงสร้าง หรือเมื่อมีการปรับปรุงระบบสารสนเทศ เป็นต้น

๒. ผู้ดูแลระบบสารสนเทศจะต้องกำหนดสิทธิในการทำลายข้อมูลในระบบให้แก่ผู้ทำลายข้อมูลตามที่เจ้าของข้อมูลกำหนด

๓. ผู้ทำลายข้อมูลต้องทำลายข้อมูลตามแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงาน

๔. กำหนดให้เจ้าของข้อมูลต้องจัดเก็บคำอธิบายชุดข้อมูลดิจิทัลหรือเมทาดาตาที่ทำลายสำหรับตรวจสอบในภายหลัง

๕. กำหนดให้ผู้ทำลายข้อมูลจัดเก็บบันทึกรายละเอียดการทำลายข้อมูลไว้ในทะเบียนควบคุมและบันทึกการทำลายข้อมูล โดยให้เก็บรักษาไว้เป็นหลักฐานไม่น้อยกว่า ๑ ปี

๖. กำหนดให้ผู้ใช้ข้อมูลส่วนบุคคลทำลายข้อมูลส่วนบุคคลเมื่อเจ้าของข้อมูลส่วนบุคคลร้องขอตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒

๗. ข้อปฏิบัติอื่นๆ ตามที่หน่วยงานกำหนดเพิ่มเติม

๖. การเชื่อมโยงและการแลกเปลี่ยนข้อมูล ในการการเชื่อมโยงและการแลกเปลี่ยนข้อมูลผู้ที่เกี่ยวข้องต้องปฏิบัติตามตามนโยบายธรรมาภิบาลข้อมูลของสำนักงาน หมวด ๖ การแลกเปลี่ยนและการเชื่อมโยง เพื่อให้การเชื่อมโยงและการแลกเปลี่ยนข้อมูลดิจิทัลทั้งภายในหน่วยงานและระหว่างหน่วยงาน มีประสิทธิภาพและก่อให้เกิดประโยชน์ต่อภาคประชาชนภาครัฐและภาคเอกชน โดยมีผู้รับผิดชอบงาน ดังนี้

- ผู้จัดการโครงการ (Project Managers)
- ผู้ดูแลระบบแม่ข่าย (Server Administrators)
- เจ้าของข้อมูล (Data Owners)
- บริกรข้อมูล (Data Stewards)
- ทีมบริหารจัดการข้อมูล (Data Management Team)

ข้อปฏิบัติ

๑. กำหนดให้ผู้จัดการโครงการกำหนดวิธีปฏิบัติและมาตรฐานทางด้านเทคนิคที่จำเป็นต้องใช้เกี่ยวกับการเชื่อมโยงและแลกเปลี่ยนข้อมูลของโครงการในความรับผิดชอบ ดังนี้

- การเชื่อมโยงและแลกเปลี่ยนข้อมูลภายในหน่วยงาน กำหนดให้ใช้รูปแบบที่เป็นมาตรฐานเปิด (Open Format) ทั้งในส่วนมาตรฐานข้อมูล เช่น XML และ JSON เป็นต้น มาตรฐานโปรโตคอลสื่อสาร เช่น SOAP REST หรืออื่น ๆ ที่ได้รับการยอมรับจากมาตรฐานสากล
- การเชื่อมโยงและแลกเปลี่ยนข้อมูลระหว่างหน่วยงาน ให้ดำเนินการตามมารตฐานกลางของหน่วยงานหลักที่เป็นผู้รับผิดชอบ

๒. กำหนดให้ผู้จัดการโครงการตรวจสอบคำอธิบายชุดข้อมูลดิจิทัลหรือเมทาดาตาที่จะทำการเชื่อมโยงและแลกเปลี่ยนให้ครบถ้วน ดังนี้

- ตรวจสอบเมทาดาตาของชุดข้อมูลดิจิทัลที่จัดเก็บให้มีฟิลด์ข้อมูลครบถ้วนสอดคล้องกับความต้องการของหน่วยงานที่ขอใช้หากไม่ครบถ้วนต้องจัดทำเพิ่มเติมตามความต้องการของหน่วยงานที่ขอใช้

- ตรวจสอบชั้นความลับของข้อมูลว่าอยู่ในชั้นความลับที่สามารถเปิดเผยได้หรือไม่ โดยต้องไม่ขัดต่อกฎหมาย ระเบียบ ข้อบังคับ ความมั่นคงของประเทศ ความลับทางราชการ และความเป็นส่วนตัว พร้อมทั้งตรวจสอบสิทธิของหน่วยงานที่สามารถนำข้อมูลไปใช้ได้ตามบทบาทและภารกิจ ตามกฎหมายของหน่วยงานนั้น ๆ

- หากไม่ครบถ้วน หรือไม่เป็นปัจจุบัน ให้แจ้งเจ้าของข้อมูล บริกรข้อมูล และทีมบริหารจัดการข้อมูลทำการจัดทำ/ปรับปรุงให้เป็นปัจจุบัน

๓. ในกรณีที่มีหน่วยงานอื่นที่ไม่มีอำนาจในการเข้าถึงข้อมูลส่วนบุคคลแต่ต้องการใช้ข้อมูลส่วนบุคคลในการครอบครองของหน่วยงาน เพื่อทำการศึกษาหรือวิจัย ซึ่งเป็นข้อยกเว้นตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ ให้หน่วยงานเจ้าของข้อมูลอนุญาตหน่วยงานนั้นในการเชื่อมโยงข้อมูลได้ โดยจะต้องแสดงข้อมูลนั้นด้วยวิธีไม่แสดงตัวตน (Anonymization)

๔. กำหนดให้มีมาตรการรักษาความมั่นคงปลอดภัยเกี่ยวกับการเชื่อมโยงและแลกเปลี่ยนข้อมูลดิจิทัล เพื่อป้องกันมิให้มีการรับส่งข้อมูลที่ไม่สมบูรณ์ หรือส่งข้อมูลไปผิดที่หรือมีการรั่วไหลของข้อมูล หรือข้อมูลถูกแก้ไขเปลี่ยนแปลง ถูกทำซ้ำใหม่ ถูกส่งซ้ำโดยมิได้รับอนุญาต

๕. ห้ามมิให้เชื่อมโยงและแลกเปลี่ยนเพื่อส่งต่อข้อมูลคอมพิวเตอร์ที่เป็นการกระทำความผิดตามกฎหมายว่าด้วยการกระทำความผิดทางคอมพิวเตอร์

๖. กำหนดให้ผู้ดูระบบแม่ข่ายต้องจัดเก็บบันทึกหลักฐานของการเชื่อมโยงและการแลกเปลี่ยนข้อมูลดิจิทัล เพื่อใช้ตรวจสอบสิ่งผิดปกติต่าง ๆ ที่เกิดขึ้นในการเชื่อมโยงและแลกเปลี่ยนข้อมูล

๗. ข้อปฏิบัติอื่น ๆ ตามที่หน่วยงานกำหนดเพิ่มเติม

ประกาศ ณ วันที่ ๑๗ กุมภาพันธ์ พ.ศ. ๒๕๖๙

(นางจินดารัตน์ วิริยะทวีกุล)
ผู้อำนวยการสำนักงานบริหารหนี้สาธารณะ

เอกสารประกอบ
การประเมินคุณภาพข้อมูล

เอกสารประกอบการประเมินคุณภาพข้อมูล

หลักเกณฑ์การประเมินคุณภาพข้อมูล (Data Quality Assessment: DQA) มีวัตถุประสงค์เพื่อใช้เป็นกรอบและเครื่องมือสำหรับตรวจสอบคุณภาพข้อมูลเบื้องต้นให้เป็นไปตามกรอบธรรมาภิบาลข้อมูลภาครัฐสอดคล้องกับภารกิจของสำนักงาน รวมทั้งสอดคล้องกับกฎหมายและระเบียบต่าง ๆ ที่เกี่ยวข้องต่อไปนี้เป็นอย่างน้อย ได้แก่

พระราชบัญญัติการบริหารงานและการให้บริการภาครัฐผ่านระบบดิจิทัล พ.ศ. ๒๕๖๒

- มาตรา ๗ (๒) กำหนดให้คณะกรรมการพัฒนารัฐบาลดิจิทัลจัดทำธรรมาภิบาลข้อมูลภาครัฐ

- มาตรา ๘ (๓) กำหนดให้ธรรมาภิบาลข้อมูลภาครัฐตามมาตรา ๗ (๒) อย่างน้อยต้องประกอบด้วยการมีมาตรการในการควบคุมและพัฒนาคุณภาพข้อมูล เพื่อให้ข้อมูลมีความถูกต้อง ครบถ้วน พร้อมใช้งาน เป็นปัจจุบัน สามารถบูรณาการและมีคุณสมบัติแลกเปลี่ยนกันได้ รวมทั้งมีการวัดผลการบริหารจัดการข้อมูลเพื่อให้หน่วยงานของรัฐมีข้อมูลที่มีคุณภาพและต่อยอดนวัตกรรมจากการใช้ข้อมูลได้

ประกาศคณะกรรมการพัฒนารัฐบาลดิจิทัล เรื่อง ธรรมาภิบาลข้อมูลภาครัฐ

- ข้อ ๔ (๓) กำหนดให้ธรรมาภิบาลข้อมูลภาครัฐในระดับหน่วยงาน ต้องประกอบด้วยเนื้อหาอย่างน้อยในเรื่องการกำหนดมาตรการควบคุมและพัฒนาคุณภาพข้อมูล เพื่อให้ข้อมูลมีความถูกต้อง ครบถ้วน เป็นปัจจุบัน มั่นคงปลอดภัย และไม่ถูกละเมิดความเป็นส่วนบุคคล รวมทั้งสามารถเชื่อมโยงแลกเปลี่ยนบูรณาการและใช้ประโยชน์ได้อย่างมีประสิทธิภาพ

- ข้อ ๔ (๔) กำหนดให้การวัดผลการบริหารจัดการข้อมูล โดยอย่างน้อยประกอบด้วยการประเมินความพร้อมของธรรมาภิบาล ข้อมูลภาครัฐในระดับหน่วยงาน การประเมินคุณภาพข้อมูลและการประเมินความมั่นคงปลอดภัยของข้อมูล

มาตรฐานรัฐบาลดิจิทัล ว่าด้วยหลักเกณฑ์การประเมินคุณภาพข้อมูลสำหรับหน่วยงานภาครัฐ (มรด. ๕ : ๒๕๖๕)

- ข้อ ๓ หลักเกณฑ์การประเมินคุณภาพข้อมูลสำหรับหน่วยงานภาครัฐ

เกณฑ์การประเมินคุณภาพข้อมูล ตามมิติคุณภาพข้อมูล ๕ มิติ ได้แก่ (๑) ความถูกต้อง (๒) ความสอดคล้องกัน (๓) ตรงตามความต้องการของผู้ใช้ (๔) ความเป็นปัจจุบัน และ (๕) ความพร้อมใช้ ที่สอดคล้องตามองค์ประกอบในการประเมินคุณภาพข้อมูลตามกรอบธรรมาภิบาลข้อมูลภาครัฐ โดยแต่ละมิติมีรายละเอียดและตัวชี้วัด (Indicators)

เครื่องมือการประเมินคุณภาพข้อมูล มีวัตถุประสงค์เพื่อให้หน่วยงานภาครัฐใช้ในการตรวจสอบและควบคุมการบริหารจัดการข้อมูลเพื่อให้ได้ข้อมูลที่มีคุณภาพ น่าเชื่อถือ รวมทั้งสามารถนำไปใช้ประโยชน์เพื่อเพิ่มประสิทธิภาพในการทำงาน เพิ่มคุณค่าในการให้บริการภาครัฐ ตลอดจนสร้างความเชื่อมั่นให้กับผู้ใช้ข้อมูลภาครัฐ ประกอบด้วย ๓ รูปแบบ ดังนี้

๑. แบบตรวจประเมินคุณภาพข้อมูล (DQA Checklist) จัดทำเพื่อให้ผู้ประเมินคุณภาพข้อมูลใช้ดำเนินการตรวจสอบกระบวนการเตรียมข้อมูลที่มีคุณภาพและคุณภาพข้อมูลใน ๕ มิติ ได้แก่ ความถูกต้องและสมบูรณ์ (Accuracy and Completeness) ความสอดคล้องกัน (Consistency) ความเป็นปัจจุบัน (Timeliness) ตรงตามความต้องการของผู้ใช้ (Relevancy) ความพร้อมใช้ (Availability) โดยการประเมินคุณภาพข้อมูล ***ผู้ประเมิน*** ควรต้องทำความเข้าใจข้อเสนอแนะสำหรับการประเมินคุณภาพข้อมูลและดำเนินการกรอกรายละเอียดในแบบฟอร์ม จากนั้นดำเนินการตรวจประเมินคุณภาพข้อมูลตามรายการในแต่ละมิติของตัวชี้วัด โดยสามารถนำผลจาก DQA Self-Assessment มาประกอบการตรวจประเมินและนำเสนอต่อผู้บริหารต่อไป

/๒. แบบประเมิน ...

๒. แบบประเมินคุณภาพข้อมูลด้วยตนเอง (DQA Self-Assessment) จัดทำเพื่อประเมินชุดข้อมูล (Data Output) ตามมิติคุณภาพข้อมูลใน ๕ มิติ ได้แก่ ความถูกต้องและสมบูรณ์ (Accuracy and Completeness) ความสอดคล้องกัน (Consistency) ความเป็นปัจจุบัน (Timeliness) ตรงตามความต้องการของผู้ใช้ (Relevancy) ความพร้อมใช้ (Availability) โดยเป็นการประเมินตนเอง (Self-assessment) เพื่อให้ทราบว่าข้อมูลภายในหน่วยงานมีคุณภาพมากน้อยเพียงใด และควรปรับปรุงหรือพัฒนาในมิติใดบ้างเพื่อให้ข้อมูลมีคุณภาพ สามารถนำไปใช้ประโยชน์เพื่อเพิ่มประสิทธิภาพในการทำงาน เพิ่มคุณค่าในการให้บริการ และต่อยอดการพัฒนาของประเทศในมิติต่าง ๆ ได้ โดยการประเมินคุณภาพข้อมูล ***เจ้าของข้อมูล (Data Owner)*** ควรพิจารณาข้อมูลภาพรวมของหน่วยงาน และทำการประเมินคุณภาพข้อมูล โดยกรอกค่าคะแนนในแต่ละมิติของตัวชี้วัด (Indicators) จากนั้นระบบจะประมวลผลตามเกณฑ์ประเมินคุณภาพข้อมูลในแต่ละมิติแสดงผลในรูปแบบ Radar Graph จัดพิมพ์แบบประเมินส่งให้ผู้ประเมินเพื่อใช้ประกอบการตรวจแบบประเมินคุณภาพข้อมูล (DQA Checklist)

๓. แบบตรวจประเมินการควบคุมและติดตามคุณภาพข้อมูล (Data Quality Monitoring and Control Checklist) จัดทำเพื่อตรวจสอบหลักฐานในการสนับสนุนกระบวนการเผยแพร่ข้อมูลที่มีคุณภาพตั้งแต่การจัดเตรียมข้อมูล การเผยแพร่ข้อมูล และการรายงานผลข้อมูล เพื่อกำหนดเป็นมาตรฐานในการดำเนินงานในหน่วยงาน โดยประเมินระดับความเสี่ยงของกระบวนการทำงาน ได้แก่ ความเสี่ยงสูง (ไม่มี) คือ ไม่มีแผนปฏิบัติงาน ความเสี่ยงปานกลาง (มีบางส่วน) คือ มีแผนปฏิบัติงานในบางขั้นตอน หรืออยู่ระหว่างการดำเนินงาน ความเสี่ยงต่ำ (มีอย่างเหมาะสม) คือ มีแผนปฏิบัติงานอย่างเป็นทางการครอบคลุมทุกขอบเขตภารกิจ/กระบวนการทำงาน ทั้งนี้ ควรมีหลักฐานแนบเพื่อสนับสนุนกระบวนการทำงานนั้นๆ พร้อมทั้งระบุรายละเอียดแผนปฏิบัติงาน (Action Plan) ซึ่งในกระบวนการทำงานที่มีความเสี่ยงสูงและความเสี่ยงปานกลาง ต้องได้รับการจัดการ/ลดความเสี่ยงดังกล่าว รวมถึงกำหนดระยะเวลาเป้าหมายที่เหมาะสมเพื่อให้สามารถลดความเสี่ยงลงได้ ซึ่งการดำเนินงานตามแผนปฏิบัติจะมีการตรวจสอบจากผู้ประเมิน/คณะกรรมการตรวจสอบและรับรองอย่างน้อยทุก ๖ เดือน โดยการประเมินคุณภาพข้อมูล ***ผู้ประเมิน/เจ้าของข้อมูล (Data Owner)*** ทำความเข้าใจคำชี้แจงและกรอกแบบตรวจประเมินให้ครบถ้วนสมบูรณ์ด้วยระบบอิเล็กทรอนิกส์ และส่งกลับให้ผู้ประเมิน/คณะกรรมการตรวจสอบผลภายในระยะเวลาที่กำหนด

ข้อเสนอแนะสำหรับการประเมินคุณภาพข้อมูล

๑. ผู้ประเมินคุณภาพข้อมูลควรตรวจสอบให้แน่ใจว่า มีความเข้าใจที่ถูกต้องตรงกันเกี่ยวกับคำจำกัดความ/คำนิยามของตัวชี้วัด และขอให้ชี้แจงประเด็นที่ยังมีความไม่ชัดเจนหรือคลุมเครือก่อนที่จะดำเนินการประเมินคุณภาพข้อมูล

๒. ผู้ประเมินคุณภาพข้อมูลควรมีเอกสารวิธีการรวบรวมข้อมูลก่อนทำการประเมิน ซึ่งข้อมูลดังกล่าวควรปรากฏอยู่ในแผนการดำเนินงานที่เป็นไปตามภารกิจของหน่วยงาน และควรมีคำอธิบายที่เป็นลายลักษณ์อักษรหรือแนวปฏิบัติที่มีการประกาศเผยแพร่ก่อนการประเมินว่าข้อมูลที่ได้รับการประเมินคุณภาพควรมีการรวบรวมข้อมูลอย่างไร

๓. ผู้ประเมินคุณภาพข้อมูลควรดำเนินการประเมินคุณภาพข้อมูลตามเกณฑ์และวิธีการตรวจประเมินตามที่เจ้าของข้อมูลกำหนด ทั้งนี้ เจ้าของข้อมูลควรกำหนดเกณฑ์และวิธีการตรวจประเมินให้ชัดเจนและชี้แจงให้ผู้ประเมินคุณภาพข้อมูลรับทราบและทำความเข้าใจให้ตรงกันก่อนทำการประเมินคุณภาพข้อมูล

๔. หน่วยงานที่ร่วมดำเนินการประเมินคุณภาพข้อมูลควรมีไฟล์วิธีการรวบรวมข้อมูลและหลักฐานที่เป็นเอกสารว่าหน่วยงานกำลังรวบรวมข้อมูลตามวิธีการดังกล่าว

/๕. ผู้ประเมิน ...

๕. ผู้ประเมินคุณภาพข้อมูลควรบันทึกชื่อและตำแหน่งของบุคลากรที่มีส่วนเกี่ยวข้องทั้งหมดในการประเมินคุณภาพข้อมูล

๖. หน่วยงานที่ร่วมดำเนินการประเมินคุณภาพข้อมูลควรสามารถให้เอกสาร เช่น กระบวนการ บุคคลที่ดำเนินการตรวจสอบความถูกต้อง วันที่ประเมิน บุคคลที่พบ/กิจกรรมที่ดำเนินการ เป็นต้น ซึ่งจะเป็นหลักฐานที่อธิบายได้ว่ามีการตรวจสอบความถูกต้องของข้อมูลที่นำมารายงาน (หมายเหตุ ควรเป็นกระบวนการที่ดำเนินการอย่างต่อเนื่อง)

๗. ผู้ประเมินคุณภาพข้อมูลควรสามารถทบทวนไฟล์/บันทึกการดำเนินงานของหน่วยงาน วิธีการรวบรวมข้อมูลที่กำหนดไว้แผนการดำเนินงาน และควรมีการระบุ/อธิบายปัญหาด้านคุณภาพข้อมูล รวมทั้งประเด็นข้อคำนึงถึงเกี่ยวกับคุณภาพข้อมูลในรายงานผลการดำเนินงาน

๘. ผู้ประเมินคุณภาพข้อมูลควรจัดทำรายงานสรุปเกี่ยวกับข้อจำกัดที่พบและแผนปฏิบัติการ ซึ่งระบุระยะเวลาดำเนินการและความรับผิดชอบเพื่อกำหนดข้อจำกัดที่ควรได้รับการจัดการ

๙. กระบวนการประเมินคุณภาพข้อมูลอาจกำหนดการทำเป็นระยะตามแต่จะตกลงกันภายในหน่วยงาน อาจเป็นรายเดือน รายไตรมาส ทุก ๖ เดือน เป็นต้น โดยผู้ประเมินคุณภาพข้อมูลควรจัดทำรายงานสรุปเกี่ยวกับข้อจำกัดที่พบและแผนปฏิบัติการซึ่งระบุระยะเวลาดำเนินการและความรับผิดชอบ เพื่อกำหนดข้อจำกัดที่ควรได้รับการจัดการและเสนอให้คณะกรรมการธรรมาภิบาลข้อมูลหรือหัวหน้าหน่วยงาน พิจารณาอนุมัติเพื่อดำเนินการตามแผนการจัดการคุณภาพข้อมูลของหน่วยงานต่อไป

ทั้งนี้ สามารถสแกน QR Code เพื่อดาวน์โหลดเอกสารเครื่องมือการประเมินคุณภาพข้อมูล และดูตัวอย่างรายงานการประเมินคุณภาพข้อมูลได้ด้านล่างนี้

เครื่องมือการประเมินคุณภาพข้อมูล

ตัวอย่างรายงานการประเมินคุณภาพข้อมูล

เอกสารประกอบ
การจัดระดับชั้นข้อมูล

เกณฑ์การจัดระดับชั้นข้อมูล

Open	Private (กระทบระดับบุคคล/องค์กร)	Confidential / sensitive (กระทบระดับบุคคล/องค์กร)	Secret / Medium Sensitive (กระทบระดับบุคคล/องค์กร)	Top secret / Highly Sensitive (กระทบระดับบุคคล/องค์กร)
เกณฑ์การพิจารณาแบ่งระดับชั้นข้อมูล (Classification Criteria)*				
ตามพระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ. ๒๕๔๐ **มาตรา ๗** หน่วยงานของรัฐต้องส่งข้อมูลข่าวสารของราชการ อย่างน้อยดังต่อไปนี้ต้องลงพิมพ์ในราชกิจจานุเบกษา **มาตรา ๙** ภายใต้บังคับมาตรา ๑๔ และมาตรา ๑๕ หน่วยงาน ของรัฐต้องจัดให้มีข้อมูลข่าวสารของราชการอย่างน้อย ดังต่อไปนี้ไว้ให้ประชาชนเข้า ตรวจดูได้ ทั้งนี้ ตามหลักเกณฑ์และวิธีการที่คณะกรรมการกำหนด	**ข้อมูลจะถูกเป็นชั้น “Private” หรือไม่** รวมถึงการเปิดเผยโดยไม่ได้รับอนุญาตหรือไม่: ✓สร้างความทุกข์ใจให้กับบุคคล ✓ละเมิดการดำเนินการที่เหมาะสมเพื่อรักษาความเชื่อใจของข้อมูลที่ให้โดยบุคคลที่สาม ✓ละเมิดข้อจำกัดทางกฎหมายในการเปิดเผยข้อมูล ✓ทำให้เกิดการสูญเสียทางการเงินหรือสูญเสียศักยภาพในการหารายได้ หรือเพื่ออำนวยความสะดวกในการได้รับผลประโยชน์ที่ไม่เหมาะสม ✓ให้ผลประโยชน์ที่ไม่เป็นธรรมแก่บุคคลหรือองค์กร	**ข้อมูลจะถูกจัดเป็นชั้น “Confidential” หรือไม่** รวมถึงการเปิดเผยโดยไม่ได้รับอนุญาตหรือไม่: ✓ส่งผลกระทบต่อความสัมพันธ์กับองค์กร/ประเทศอื่นในทางลบ ✓ก่อให้เกิดความทุกข์ใจอย่างมากต่อบุคคล ✓ทำให้เกิดการสูญเสียทางการเงินหรือการสูญเสียศักยภาพในการหารายได้หรือเพื่ออำนวยความสะดวกในการได้รับผลประโยชน์หรือความได้เปรียบที่ไม่เหมาะสมสำหรับบุคคลหรือองค์กรหรือประเทศ ✓ฝ่าฝืนการดำเนินการที่เหมาะสมเพื่อรักษาความมั่นใจของข้อมูลที่ให้โดยบุคคลที่สาม	**ข้อมูลจะถูกจัดเป็นชั้น “Secret” หรือไม่** รวมถึงการเปิดเผยโดยไม่ได้รับอนุญาตหรือไม่: ✓สร้างความเสียหายอย่างมีนัยสำคัญต่อความสัมพันธ์กับองค์กรอื่น ๆ (เช่น ก่อให้เกิดการประท้วงอย่างเป็นทางการหรือการลงโทษ) ✓สร้างความเสียหายต่อประสิทธิภาพการดำเนินงานหรือความปลอดภัยขององค์กร/ประเทศ ✓ภารกิจงานสำคัญที่กระทบต่อด้านการเงินขององค์กร หรือผลประโยชน์ทางเศรษฐกิจและการค้าของประเทศ ✓บ่อนทำลายศักยภาพทางการเงินส่วนใหญ่ขององค์กร/ประเทศ	ตามตามพระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ. ๒๕๔๐ **มาตรา ๑๔** ข้อมูลข่าวสารของราชการที่อาจก่อให้เกิดความเสียหายต่อสถาบันพระมหากษัตริย์จะเปิดเผยมิได้ **มาตรา ๑๕** ข้อมูลข่าวสารของราชการหน่วยงานของรัฐหรือเจ้าหน้าที่ของรัฐอาจมีคำสั่งมิให้เปิดเผยก็ได้ โดยคำนึงถึงการปฏิบัติ หน้าที่ตามกฎหมาย ประโยชน์สาธารณะ และ ประโยชน์ของเอกชนที่เกี่ยวข้องประกอบกัน ✓ข้อมูลจะถูกจัดเป็นชั้น “Top Secret” หรือไม่ รวมถึงการเปิดเผยโดยไม่ได้รับอนุญาตหรือไม่: ✓ก่อให้เกิดความเสียหายต่อความมั่นคงของประเทศ ความสัมพันธ์ระหว่างประเทศ และความมั่นคงในทางเศรษฐกิจหรือการคลังของประเทศ

/Open ...

Open	Private (กระทบระดับบุคคล/องค์กร)	Confidential / sensitive (กระทบระดับบุคคล/องค์กร)	Secret / Medium Sensitive (กระทบระดับบุคคล/องค์กร)	Top secret / Highly Sensitive (กระทบระดับบุคคล/องค์กร)
เกณฑ์การพิจารณาแบ่งระดับชั้นข้อมูล (Classification Criteria)*				
	✓สูญเสียความได้เปรียบขององค์กรเชิงพาณิชย์หรือนโยบายในการเจรจากับผู้อื่น	✓ขัดขวางการพัฒนาที่มีประสิทธิภาพหรือการดำเนินงานตามนโยบายขององค์กร ✓ฝ่าฝืนข้อจำกัดทางกฎหมายในการเปิดเผยข้อมูล ✓สูญเสียความได้เปรียบขององค์กรเชิงพาณิชย์หรือนโยบายในการเจรจากับผู้อื่น ✓บ่อนทำลายการจัดการที่เหมาะสมและการดำเนินงานขององค์กร	✓ขัดขวางการพัฒนาหรือการดำเนินงาน ของนโยบายองค์กร/ประเทศอย่างจริงจัง ✓ปิดตัวลงหรือขัดขวางการดำเนินงาน/โครงการที่สำคัญขององค์กร/ประเทศ	✓ทำให้การบังคับใช้กฎหมายเสื่อมประสิทธิภาพ หรือไม่อาจสำเร็จตามวัตถุประสงค์ได้ ไม่ว่าจะเกี่ยวกับการฟ้องคดี การป้องกัน การปราบปราม การทดสอบ การตรวจสอบ หรือการรู้แหล่งที่มาของข้อมูลข่าวสารหรือไม่ก็ตาม ✓ความเห็นหรือคำแนะนำภายในหน่วยงานของรัฐในการดำเนินการเรื่องหนึ่งเรื่องใด แต่ทั้งนี้ไม่รวมถึงรายงานทางวิชาการ รายงานข้อเท็จจริง หรือข้อมูลข่าวสารที่นำมาใช้ในการทำความเห็นหรือคำแนะนำภายในดังกล่าว ✓การเปิดเผยจะก่อให้เกิดอันตรายต่อชีวิตหรือความปลอดภัยของบุคคลหนึ่งบุคคลใด ✓ข้อมูลข่าวสารของราชการที่มีกฎหมายคุ้มครองมิให้เปิดเผย หรือข้อมูลข่าวสารที่มีผู้ให้มาโดยไม่ประสงค์ให้ทางราชการนำไปเปิดเผยต่อผู้อื่น

หมายเหตุ เกณฑ์การพิจารณาแบ่งระดับชั้นข้อมูล ได้พิจารณาจากผลกระทบ (Impact) ทั้งด้านภาพลักษณ์/ชื่อเสียง (Reputation) ผู้ใช้บริการและการดำเนินงานตามภารกิจ (Users & Operations) การเงินและสินทรัพย์ (Financial & Assets) ความสอดคล้องกับกฎระเบียบ ข้อบังคับ (Legal & Regulation) โดยไม่มีการจำกัดเงื่อนไขเกณฑ์การพิจารณาการจัดระดับชั้นข้อมูล

/การ ...

การจัดระดับชั้นข้อมูลจะส่งผลให้ข้อมูลได้รับการดูแล โดยสามารถกำหนดเงื่อนไขการเข้าถึงข้อมูลได้ดังตัวอย่างต่อไปนี้

Open	Private (กระทบระดับบุคคล/องค์กร)	Confidential / sensitive (กระทบระดับบุคคล/องค์กร)	Secret / Medium Sensitive (กระทบระดับบุคคล/องค์กร)	Top secret / Highly Sensitive (กระทบระดับบุคคล/องค์กร)
การเข้าถึง (Access Control)				
ไม่มีการจำกัดการเข้าถึงข้อมูล/เปิดเผยสู่สาธารณะ	**เจ้าหน้าที่ส่วนใหญ่ขององค์กร** มีแนวโน้มที่จะจัดการกับข้อมูล “Private" ในระหว่างการทำงาน/เปิดเผยเมื่อได้รับอนุญาต	ได้รับการจัดการโดย **ผู้บริหารระดับกลางขึ้นไป** โดยที่เจ้าหน้าที่บางคนที่มีระดับต่ำกว่าจะได้รับการเข้าถึงเฉพาะในบางสถานการณ์เท่านั้น/เปิดเผยเมื่อได้รับอนุญาต	ต้องได้รับการควบคุมอย่างเข้มงวดโดย **ผู้บริหารระดับสูง** และในหลายกรณี จะมีการแจกจ่ายสำเนาเอกสารตามระเบียบขั้นตอนเฉพาะขององค์กรและ/หรือประเทศ/เปิดเผยเมื่อได้รับอนุญาต	คำสั่งมิให้เปิดเผยข้อมูลข่าวสารของราชการสามารถกำหนดเงื่อนไขได้ **แต่ต้องระบุว่าที่ เปิดเผยไม่ได้/ปกปิดเพราะเป็นข้อมูล ข่าวสารประเภทใดและเพราะเหตุใด** และให้ถือว่าการมีคำสั่งเปิดเผยข้อมูลข่าวสารของราชการ **เป็นดุลพินิจของเจ้าหน้าที่ของรัฐ ตามลำดับสายการบังคับบัญชา** แต่อาจอุทธรณ์ต่อคณะกรรมการวินิจฉัยการเปิดเผยข้อมูลข่าวสารได้

/ตัวอย่าง ...

ตัวอย่างการจัดระดับชั้นข้อมูล

ระดับชั้นข้อมูล / การบริหารจัดการ	เปิดเผย (Open)	เผยแพร่ภายในองค์กร (Private)	ลับ (Confidential/Sensitive)	ลับมาก (Secret/Medium sensitive)	ลับที่สุด (Top secret/Highly sensitive)
ตัวอย่างชุดข้อมูล	- กฎ มติ ค.ร.ม. ข้อบังคับ - รายงานผลการศึกษาทาง วิชาการ - ข้อมูลเปิดภาครัฐ	- ข้อมูลระเบียน - ข้อมูลพนักงาน - เอกสารประกอบการปฏิบัติงาน - วิธีปฏิบัติภายในหน่วยงาน	- ข้อมูลการฟ้องคดี - ความเห็นภายในหน่วยงานที่ยังไม่ได้ข้อยุติ	- รายงานการแพทย์ - ข้อมูลความสัมพันธ์ระหว่างประเทศ - นโยบายสำคัญที่ใช้ปฏิบัติต่อรัฐต่างประเทศ	- ข่าวสารที่อาจก่อความเสียหายต่อสถาบันพระมหากษัตริย์ - ข้อมูลที่กระทบต่อความมั่นคงทางทหาร เช่น คลังอาวุธ และความมั่นคงทางทรัพยากร เช่น ตำแหน่งของชนิดพันธุ์ที่ใกล้สูญพันธุ์/ถูกคุกคาม
การควบคุมการเข้าถึง (Access Control)	- ไม่มีการจำกัดการเข้าถึงข้อมูล/เปิดเผยสู่สาธารณะ	- จำกัดการเข้าถึงข้อมูลเฉพาะบุคคลภายในหน่วยงาน	- จำกัดการเข้าถึงเฉพาะบุคคลที่จำเป็นต้องรู้หรือมีสิทธิ์รู้โดยและลงนามข้อตกลงไม่เปิดเผยข้อมูล (non-disclosure agreements) - สามารถตรวจสอบคำขอการเข้าถึงข้อมูล การทบทวน การอนุมัติ และกระบวนการยกเลิกได้	- จำกัดการเข้าถึงเฉพาะบุคคลที่จำเป็นต้องรู้หรือมีสิทธิ์รู้โดยและลงนามข้อตกลงไม่เปิดเผยข้อมูล (non-disclosure agreements) - ต้องได้รับการอนุญาตจากเจ้าของข้อมูล	- ไม่เปิดเผย/ปกปิด

/ระดับ ...

ระดับชั้นข้อมูล / การบริหารจัดการ	เปิดเผย (Open)	เผยแพร่ภายในองค์กร (Private)	ลับ (Confidential/Sensitive)	ลับมาก (Secret/Medium sensitive)	ลับที่สุด (Top secret/Highly sensitive)
				- สามารถตรวจสอบคำขอการเข้าถึงข้อมูล การทบทวน การอนุมัติ และกระบวนการยกเลิกได้	
การเข้ารหัส (Encryption)	- ไม่มีการเข้ารหัสการ	- ไม่มีการเข้ารหัสการสร้าง การจัดเก็บ การประมวลผล และการส่งข้อมูล - มีการเข้ารหัสสำหรับบุคคลที่สาม	- การเข้ารหัสระหว่างการสร้าง การจัดเก็บ การประมวลผล และการส่งข้อมูล - มีการเข้ารหัสสำหรับบุคคลที่สาม	- มีการเข้ารหัสที่ซับซ้อนระหว่างการสร้าง การจัดเก็บ การประมวลผล และการส่งข้อมูล - มีการเข้ารหัสที่ซับซ้อนสำหรับบุคคลที่สาม	- ไม่เปิดเผย/ปกปิด
การจัดเก็บ (Storage)	- ไม่มีข้อจำกัดการจัดเก็บข้อมูล	- การจัดเก็บข้อมูลเป็นไปตามนโยบายองค์กรหรือดุลยพินิจของผู้จัดการหรือผู้คุ้มครองข้อมูล	- ห้ามจัดเก็บข้อมูลที่ลับมากในเครื่องและอุปกรณ์คอมพิวเตอร์โดยไม่ได้รับอนุญาต	- ห้ามจัดเก็บข้อมูลที่ลับมากในเครื่องและอุปกรณ์คอมพิวเตอร์โดยไม่ได้รับอนุญาต เว้นแต่จะได้รับอนุมัติจากเจ้าหน้าที่รักษาความปลอดภัยข้อมูล และ ต้องมีการเข้ารหัส - จัดเก็บที่ปลอดภัยเมื่อไม่ใช้งาน	- ไม่เปิดเผย/ปกปิด

/หลักเกณฑ์ ...

หลักเกณฑ์การการจัดระดับชั้นข้อมูล พิจารณาการจัดหมวดหมู่ของข้อมูลเป็นไปตามกรอบธรรมมาภิบาลข้อมูลภาครัฐสอดคล้องตามแนวมาตรฐานสากลและเป็นไปตามข้อกำหนดกฎหมายที่เกี่ยวข้อง โดยแบ่งระดับชั้นความลับแบ่งออกเป็น ชั้นเปิดเผย (Open) สู่สาธารณะ เปิดเผยเมื่อได้รับอนุญาต ได้แก่ ชั้นเผยแพร่ภายในองค์กร (Private) ชั้นลับ (Confidential) และ ชั้นลับมาก (Secret) เปิดเผยไม่ได้/ปกปิดได้แก่ ชั้นลับที่สุด (Top Secret) ซึ่งเจ้าของข้อมูลร่วมกับศูนย์ข้อมูลและเทคโนโลยีสารสนเทศควรเป็นผู้ประเมิน ทั้งนี้ สามารถดำเนินการจัดระดับชั้นข้อมูล ได้ดังนี้

๑. ประเมินชุดข้อมูลตามเกณฑ์การพิจารณาแบ่งระดับชั้นความลับเทียบกับระดับผลกระทบ (รวมถึงผลประโยชน์แห่งชาติ) จากการเปิดเผยข้อมูลโดยไม่ได้อนุญาต ตามหลักการระดับผลกระทบตามวัตถุประสงค์ด้านความปลอดภัยของข้อมูล (CIA) โดยใช้แผนผังการตัดสินใจจัดระดับชั้นข้อมูลเทียบกับผลกระทบจากการเปิดเผยข้อมูลโดยไม่ได้รับอนุญาต (Decision tree) เพื่อประกอบการพิจารณาจำแนกระดับชั้นความลับ

ระดับผลกระทบตามวัตถุประสงค์ด้านความปลอดภัยของข้อมูล (CIA)

วัตถุประสงค์ด้านความปลอดภัย (Security Objective)	**ผลกระทบ (Impact)* และ ผลประโยชน์แห่งชาติ (National Interests)**		
	น้อย (Low)	**ปานกลาง (Moderate)**	**สูง (High)**
ด้านความลับ (Confidentaility) การรักษาข้อจำกัดในการได้รับอนุญาตให้เข้าถึงได้และเปิดเผยเฉพาะผู้มีสิทธิ์ รวมทั้งวิธีการคุ้มครองความเป็นส่วนตัว (privacy) และกรรมสิทธิ์ (proprietary) ของข้อมูลข่าวสาร	การเปิดเผยข้อมูลโดยไม่ได้รับอนุญาตอาจส่งผลกระทบน้อย/อย่างจำกัด (limited) และเกิดผลประโยชน์แห่งชาติสำคัญน้อย (Less Important or Secondary National Interests)	การเปิดเผยข้อมูลโดยไม่ได้รับอนุญาตอาจส่งผลกระทบอย่างร้ายแรง (serious) และเกิดผลประโยชน์แห่งชาติที่สำคัญ (Important National Interests)	การเปิดเผยข้อมูลโดยไม่ได้รับอนุญาตอาจส่งผลกระทบอย่างร้ายแรงมาก (severe or catastrophic) และเกิดผลประโยชน์แห่งชาติสำคัญยิ่ง (Extremely Important National Interests)
ด้านความถูกต้อง ครบถ้วนสมบูรณ์ ความคงสภาพ (Integrity) การปกป้องจากการดัดแปลงหรือ ทำลายข้อมูลที่ไม่เหมาะสม และรวมถึงการรับรองว่าข้อมูลจะไม่ถูกปฏิเสธ (non-repudiation) และเป็นข้อมูลที่ถูกต้องเป็นความจริง (authenticity)	การแก้ไขหรือทำลายข้อมูลโดยไม่ได้รับอนุญาตอาจส่งผลกระทบน้อย/อย่างจำกัด (limited) และเกิดผลประโยชน์แห่งชาติสำคัญน้อย (Less Important or Secondary National Interests)	การแก้ไขหรือทำลายข้อมูลโดยไม่ได้รับอนุญาตอาจส่งผลกระทบอย่างร้ายแรง (serious) และเกิดผลประโยชน์แห่งชาติที่สำคัญ (Important National Interests)	การแก้ไขหรือทำลายข้อมูลโดยไม่ได้รับอนุญาตอาจส่งผลกระทบอย่างร้ายแรงมาก (severe or catastrophic) และเกิดผลประโยชน์แห่งชาติสำคัญยิ่ง (Extremely Important National Interests)

/วัตถุประสงค์ ...

วัตถุประสงค์ด้านความปลอดภัย (Security Objective)	ผลกระทบ (Impact)* และ ผลประโยชน์แห่งชาติ (National Interests)		
	น้อย (Low)	ปานกลาง (Moderate)	สูง (High)
ด้านความพร้อมใช้งาน (Availability) การสร้างความมั่นใจในการเข้าถึง และการใช้ข้อมูลอย่างทันท่วงที/เป็นปัจจุบัน และเชื่อถือได้	การหยุดชะงักของการเข้าถึง หรือการใช้ข้อมูลข่าวสารหรือระบบสารสนเทศอาจส่งผลกระทบน้อย/อย่างจำกัด (limited) และเกิดผลประโยชน์แห่งชาติสำคัญน้อย (Less Important or Secondary National Interests)	การหยุดชะงักของการเข้าถึง หรือการใช้ข้อมูลข่าวสารหรือระบบสารสนเทศอาจส่งผล กระทบอย่างร้ายแรง (serious) และเกิดผลประโยชน์แห่งชาติที่สำคัญ (Important National Interests)	การหยุดชะงักของการเข้าถึง หรือการใช้ข้อมูลข่าวสาร หรือระบบสารสนเทศอาจส่งผลกระทบอย่างร้ายแรงมาก (severe or catastrophic) และเกิดผลประโยชน์แห่งชาติสำคัญยิ่ง (Extremely Important National Interests)

ในการประเมินระดับผลกระทบตามวัตถุประสงค์ด้านความปลอดภัยของข้อมูล (CIA) สามารถประเมินจากแผนผังการตัดสินใจจัดระดับชั้นข้อมูลเทียบกับผลกระทบจากการเปิดเผยข้อมูลโดยไม่ได้รับอนุญาต (Decision tree) รวมถึงผลประโยชน์แห่งชาติ (National Interest) ทั้งนี้ สามารถสแกน QR Code เพื่อดาวน์โหลดเอกสารประกอบการประเมินได้ด้านล่างนี้

Decision tree

National Interest

/๒. การประเมิน ...

๒. การประเมินความเสี่ยงและผลกระทบของการเปิดเผยข้อมูลโดยไม่ได้รับอนุญาต โดยพิจารณาเงื่อนไขในการกำหนดเกณฑ์การประเมินความเสี่ยงใน ๒ มิติ คือ มิติแรก โอกาสที่จะเกิดความเสี่ยง (Likelihood) และ มิติที่สอง ผลกระทบ (Impact) เพื่อกำหนดระดับความเสี่ยง (Level of Risk) การวิเคราะห์ความเสี่ยงสามารถเป็นได้ทั้งการวิเคราะห์เชิงคุณภาพ (Qualitative) กึ่งปริมาณ (Semi-Quantitative) เชิงปริมาณ (Quantitative) หรือผสมผสานกันไปกระบวนการประเมินความเสี่ยงของหน่วยงาน จะทำการวิเคราะห์โอกาสที่จะเกิดเหตุการณ์ความเสี่ยงและผลกระทบอันเนื่องมาจากความเสี่ยง

๒.๑ โอกาสที่จะเกิด (Likelihood) หมายถึง การประเมินโอกาสความเสี่ยงจากการเปิดเผยข้อมูล โดยไม่ได้รับอนุญาตหรือการรั่วไหลของข้อมูลที่มีระดับชั้นความลับที่จะเกิดขึ้น โดยการพิจารณาจากสถิติการเกิด เหตุการณ์ในอดีต ปัจจุบัน หรือการคาดการณ์ล่วงหน้าของโอกาสที่จะเกิดในอนาคต ทั้งนี้ให้ผู้ดูแลข้อมูลและเจ้าของข้อมูลร่วมกันประเมินโอกาสที่จะเกิดขึ้น โดยมีระดับคะแนนและระดับความเสี่ยงดังนี้

ระดับคะแนน	ความหมาย
๕	มีโอกาสเกิดขึ้นสูงมาก/เป็นประจำ
๔	มีโอกาสเกิดขึ้นสูง/บ่อยครั้ง
๓	มีโอกาสเกิดขึ้นบ้าง/บางครั้ง
๒	มีโอกาสเกิดขึ้นน้อยครั้ง
๑	มีโอกาสเกิดขึ้นยาก

๒.๒ ผลกระทบ (Impact) หมายถึง ความเสียหายที่จะเกิดขึ้นหากความเสี่ยงนั้นเกิดขึ้น เป็นการพิจารณาระดับความรุนแรงและมูลค่าความเสียหายจากความเสี่ยงที่คาดว่าจะได้รับ โดยมีระดับคะแนนและเกณฑ์การพิจารณาระดับผลกระทบและผลประโยชน์แห่งชาติ ดังนี้

ระดับคะแนน	ความหมาย
๓	ความรุนแรงของผลกระทบระดับสูง
๒	ความรุนแรงของผลกระทบระดับปานกลาง
๑	ความรุนแรงของผลกระทบระดับน้อย

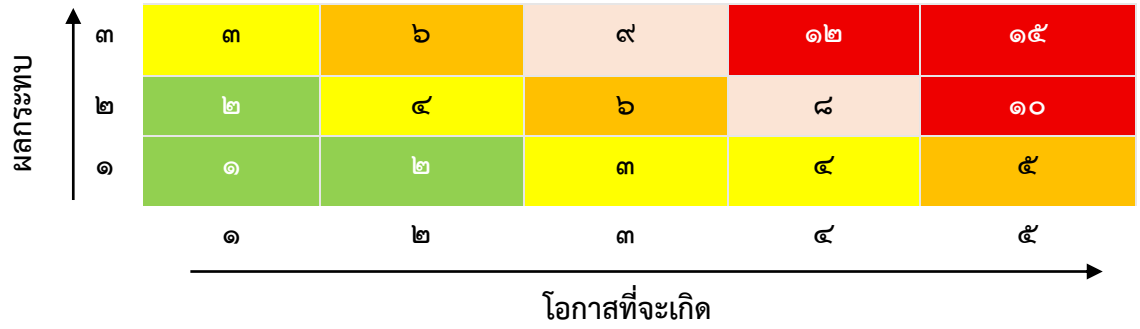
เกณฑ์การพิจารณาระดับผลกระทบและผลประโยชน์แห่งชาติ

เกณฑ์	ค่าคะแนนระดับความรุนแรงของระดับผลกระทบและผลประโยชน์แห่งชาติ		
	๑ = น้อย	๒ = ปานกลาง	๓ = สูง
ภาพลักษณ์/ชื่อเสียง (Reputation)	น้อย/อย่างจำกัด	อย่างร้ายแรง	อย่างร้ายแรงมาก
ผู้ใช้และการดำเนินงาน (Users & Operations)	รายบริการ/การดำเนินงานขององค์กร	รายกลุ่มบริการ/การดำเนินของกระทรวง/ระหว่างองค์กร/จังหวัด	ข้ามกลุ่มบริการ/ภูมิภาค การดำเนินงานตามแผนบูรณาการ/กลุ่มจังหวัด
การเงินและสินทรัพย์ (Financial & Assets)	ตั้งแต่ ๕ แสน แต่ไม่เกิน ๕ ล้าน/ Small project	ตั้งแต่ ๕ ล้าน แต่ไม่เกิน ๕๐ ล้าน/ Medium project	ตั้งแต่ ๕๐ ล้าน แต่ไม่เกิน ๑๐๐ ล้าน/ Large Project

/เกณฑ์ ...

เกณฑ์	ค่าคะแนนระดับความรุนแรงของระดับผลกระทบและผลประโยชน์แห่งชาติ		
	๑ = น้อย	๒ = ปานกลาง	๓ = สูง
กฎหมายและระเบียบ (Legal and Regulation)	ละเว้นการปฏิบัติตามระเบียบ ข้อบังคับขององค์กร ซึ่งเกิดผลกระทบน้อย	ละเว้นการปฏิบัติตามระเบียบ ข้อบังคับและกฎกระทรวง ซึ่งเกิดผลกระทบที่มีนัยสำคัญ และไม่เป็นไปตามเป้าของ ก.พ.ร.	ละเว้นการปฏิบัติตามกฎหมาย มติ ครม. หรือระเบียบข้อบังคับ ซึ่งเกิดผลกระทบที่มีนัยสำคัญ และไม่เป็นไปตามเป้าของแผนบูรณาการ/กลุ่มจังหวัด
ผลประโยชน์แห่งชาติ (ค่าเฉลี่ย CIA) (National Interests)	ผลประโยชน์แห่งชาติสำคัญน้อย	ผลประโยชน์แห่งชาติที่สำคัญ	ผลประโยชน์แห่งชาติที่สำคัญยิ่ง

๒.๓ ระดับความเสี่ยง (Risk Level) กำหนดค่าเท่ากับผลคูณของระดับโอกาสที่ความเสี่ยงอาจเกิดขึ้น (Likelihood) และระดับความรุนแรงของผลกระทบ (Impact) อันเนื่องมาจากความเสี่ยง ซึ่งระดับความเสี่ยงแบ่งตามความสำคัญและการจัดการความเสี่ยงได้ดังนี้



ค่าระดับความเสี่ยง	ระดับความเสี่ยง	ความหมาย
๑-๒	ต่ำมาก	ระดับความเสี่ยงที่องค์กรสามารถยอมรับได้ โดยไม่ต้องมีมาตรการควบคุม
๓-๔	ต่ำ	ระดับความเสี่ยงที่องค์กรสามารถยอมรับได้ โดยมีมาตรการควบคุมอยู่แล้วหรือไม่ก็ได้ แต่อาจต้องมีการติดตามเป็นระยะ ๆ
๕-๖	ปานกลาง	ระดับความเสี่ยงที่องค์กรสามารถยอมรับได้โดยต้องมีมาตรการควบคุมหรือมีแผนการลดความเสี่ยง เพื่อลดความเสี่ยงให้ไปอยู่ในระดับต่ำและป้องกันไม่ให้ความเสี่ยงเพิ่มขึ้น

/ค่าระดับ ...

ค่าระดับความเสี่ยง	ระดับความเสี่ยง	ความหมาย
๗-๙	**สูง**	ระดับความเสี่ยงที่องค์กรไม่สามารถยอมรับได้ และต้องจัดการลดความเสี่ยงให้ไปอยู่ในระดับต่ำลงโดยเร็ว โดยต้องจัดให้มีแผนการลดความเสี่ยงและป้องกันไม่ให้ความเสี่ยงกลับเพิ่มสูงขึ้นด้วย
๑๐ ขึ้นไป	**สูงมาก**	ระดับความเสี่ยงที่องค์กรไม่สามารถยอมรับได้ และต้องจัดการลดความเสี่ยงให้ไปอยู่ในระดับต่ำลงในทันที หรืออาจมีการถ่ายโอนความเสี่ยง โดยต้องจัดให้มีแผนการลดความเสี่ยงและป้องกันไม่ให้ความเสี่ยงกลับเพิ่มสูงขึ้นด้วย

๒.๔ ติดป้ายหรือแท็กกำกับระดับชั้นข้อมูลตามความอ่อนไหว ความเสี่ยงและผลกระทบจากการเปิดเผยข้อมูลโดยไม่ได้รับอนุญาต

ระดับชั้นข้อมูล (Data Classification Level)	ระดับผลกระทบโดยรวม (Overall Impact Level)	ระดับความเสี่ยงโดยรวม (Overall Risk Level)
เปิดเผย (Open)	น้อยมาก (Very Low)	ต่ำมาก (Very Low)
เผยแพร่ภายในองค์กร (Private)	น้อย (Low)	ต่ำ (Low)
ลับ (Confidential / Sensitive)	ปานกลาง (Moderate)	ปานกลาง (Moderate)
ลับมาก (Secret / Medium Sensitive)	สูง (High)	สูง (High)
ลับที่สุด (Top secret / Highly Sensitive)	สูงมาก (Very High)	สูงมาก (Very High)

ทั้งนี้ สามารถสแกน QR Code เพื่อดาวน์โหลดเอกสารประกอบการประเมินได้ด้านล่างนี้

แบบฟอร์ม
การจัดระดับชั้นข้อมูลภาครัฐ

ตัวอย่าง
การจัดระดับชั้นข้อมูลภาครัฐ

เอกสารประกอบ
การบริหารจัดการข้อมูล

ตารางแสดงความสัมพันธ์ระหว่างกระบวนการ/กิจกรรมและผู้มีส่วนได้ส่วนเสีย

ตารางที่: ๑ ตัวอย่างผู้มีส่วนได้ส่วนเสียในการสร้างข้อมูล

กิจกรรม	ผู้มีส่วนได้ส่วนเสีย				
	ผู้สร้างข้อมูล	ทีมบริหารจัดการข้อมูล	เจ้าของข้อมูล	บริกรข้อมูล	ผู้ดูแลระบบสารสนเทศ
กำหนดผู้มีสิทธิในการสร้างข้อมูลและกำหนดหมวดหมู่และชั้นความลับ	I	I	R	C	S
กำหนดสิทธิในการสร้างข้อมูลในระบบให้แก่ผู้สร้างข้อมูล	I	I	S	I	R
สร้างข้อมูลที่ไม่ขัดต่อกฎหมายและจากแหล่งข้อมูลที่เชื่อถือได้เท่านั้น	R	I	C	C	S
จัดทำคำอธิบายชุดข้อมูลดิจิทัล	S	S	R	R	S
ประเมินคุณค่าของชุดข้อมูลดิจิทัล	I	I	R	R	I
ตรวจสอบความถูกต้องของข้อมูล	I	I	R	R	I

ตารางที่: ๒ ตัวอย่างผู้มีส่วนได้ส่วนเสียในการจัดเก็บข้อมูล

กิจกรรม	ผู้มีส่วนได้ส่วนเสีย					
	เจ้าของข้อมูล	ผู้ดูแลระบบสารสนเทศ	ผู้สร้างข้อมูล	ผู้ใช้ข้อมูล	บริกรข้อมูล	ทีมบริหารจัดการข้อมูล
กำหนดระยะเวลาในการจัดเก็บข้อมูล	R	S	S	I	I	S
ย้ายข้อมูลที่มีการจัดเก็บเกินระยะเวลาที่กำหนด	I	R	I	I	I	R
จัดทำคำอธิบายชุดข้อมูลดิจิทัลและปรับปรุงให้เป็นปัจจุบัน	R	S	S	I	R	R
จัดเก็บข้อมูลตามการจัดชั้นความลับของหน่วยงาน	R	S	R	I	C	S
จัดเก็บข้อมูลส่วนบุคคลเท่าที่จำเป็น	R	S	S	R	C	S
ยกเลิกการจัดเก็บข้อมูลส่วนบุคคลกรณีเจ้าของข้อมูลส่วนบุคคลถอนความยินยอม	R	R	I	R	I	I
จัดเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์	I	R	I	I	I	I

/ตารางที่: ๓ ...

ตารางที่: ๓ ตัวอย่างผู้มีส่วนได้ส่วนเสียในการประมวลผลและใช้ข้อมูล

กิจกรรม	**ผู้มีส่วนได้ส่วนเสีย**		
	เจ้าของข้อมูล	ผู้ใช้ข้อมูล	ผู้ดูแลระบบสารสนเทศ
กำหนดสิทธิในการประมวลผลและใช้งานข้อมูลตามชั้นความลับ	R	I	I
กำหนดสิทธิในการประมวลผลและเข้าใช้งานข้อมูลในระบบ	C	I	R
ไม่ใช้ข้อมูลในเครือข่ายของหน่วยงานเพื่อประโยชน์ในเชิงธุรกิจเป็นการส่วนตัว	C	R	S
ประมวลผลข้อมูลหรือใช้ข้อมูลส่วนบุคคลเท่าที่จำเป็น	C	R	S
ยกเลิกการประมวลผลข้อมูลหรือการใช้ข้อมูลส่วนบุคคล กรณีที่เจ้าของข้อมูลส่วนบุคคลถอนความยินยอม	C	R	S

ตารางที่: ๔ ตัวอย่างผู้มีส่วนได้ส่วนเสียในการเปิดเผยข้อมูล

กิจกรรม	**ผู้มีส่วนได้ส่วนเสีย**			
	เจ้าของข้อมูล	ผู้ใช้ข้อมูล	บริกรข้อมูล	ทีมบริหารจัดการข้อมูล
จะต้องเปิดเผยข้อมูลในความรับผิดชอบต่อสาธารณะตามกฎหมาย/มาตรฐานที่เกี่ยวข้อง	R	I	C	S
คัดเลือกข้อมูลที่จะเปิดเผยในรูปแบบข้อมูลเปิดจากลำดับชั้นความสำคัญของ High Value Dataset	R	I	C	S
ตรวจสอบคำอธิบายชุดข้อมูลดิจิทัลที่จะทำการเปิดเผยให้มีความครบถ้วนเป็นปัจจุบัน	R	I	R	R
เปิดเผยข้อมูลส่วนบุคคลตามข้อกำหนดของพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ และห้ามเปิดเผยข้อมูลความมั่นคงและข้อมูลความลับทางราชการ รวมถึงข้อมูลที่เป็นการกระทำความผิดตามกฎหมาย	R	R	C	S
กำหนดรอบระยะเวลาในการตรวจสอบและปรับปรุงข้อมูลที่เปิดเผย	R	I	I	I

/ตารางที่: ๕ ...

ตารางที่: ๕ ตัวอย่างผู้มีส่วนได้ส่วนเสียในการทำลายข้อมูล

กิจกรรม	**ผู้มีส่วนได้ส่วนเสีย**			
	เจ้าของข้อมูล	ผู้ดูแลระบบสารสนเทศ	ผู้ทำลายข้อมูล	ผู้ใช้ข้อมูล
กำหนดผู้มีสิทธิในการทำลายข้อมูล	R	R	I	I
ทำลายข้อมูลตามแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงาน	C	S	R	I
จัดเก็บคำอธิบายข้อมูลที่ทำลายสำหรับตรวจสอบในภายหลัง	R	S	R	I
จัดเก็บบันทึกรายละเอียดการทำลายข้อมูล	I	S	R	I
ทำลายข้อมูลส่วนบุคคลเมื่อเจ้าของข้อมูลส่วนบุคคลร้องขอพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒	C	S	I	R

ตารางที่: ๖ ตัวอย่างผู้มีส่วนได้ส่วนเสียในการเชื่อมโยงและแลกเปลี่ยนข้อมูล

กิจกรรม	**ผู้มีส่วนได้ส่วนเสีย**				
	ผู้จัดการโครงการ	ผู้ดูแลระบบแม่ข่าย	เจ้าของข้อมูล	บริกรข้อมูล	ทีมบริหารจัดการข้อมูล
กำหนดวิธีปฏิบัติและมาตรฐานทางด้านเทคนิคจำเป็นในการเชื่อมโยงและแลกเปลี่ยนข้อมูลของโครงการ	R	S	I	I	I
ตรวจสอบคำอธิบายชุดข้อมูลดิจิทัลและชั้นความลับของข้อมูล	R	R	C	C	S
จัดทำแนวทางการทำงานร่วมกันทั้งระหว่างหน่วยงานภายในและหน่วยงานภายนอกในการเชื่อมโยงและแลกเปลี่ยนข้อมูล	R	S	S	S	S
จัดเก็บบันทึกหลักฐานของการเชื่อมโยงและการแลกเปลี่ยนข้อมูลดิจิทัล	I	R	I	I	I

หมายเหตุ

R (Responsible) หมายถึง ผู้มีหน้าที่ในการปฏิบัติงานตามกระบวนการหรือกิจกรรมที่กำหนดไว้

A (Accountable) หมายถึง ผู้มีหน้าที่ในการทบทวนและอนุมัติผลที่ได้รับจากปฏิบัติงาน

S (Supportive) หมายถึง ผู้ที่มีหน้าที่ในการสนับสนุนหรือให้การช่วยเหลือต่อปฏิบัติงาน

C (Consulted) หมายถึง ผู้ที่ทำหน้าที่ให้คำปรึกษาต่อผู้ปฏิบัติงาน

I (Informed) หมายถึง ผู้ที่ทำหน้าที่รับทราบผลการปฏิบัติงาน