นโยบายธรรมาภิบาลข้อมูลของกรมราชทัณฑ์ พ.ศ. 2568

ศูนย์เทคโนโลยีสารสนเทศ

กองยุทธศาสตร์และแผนงาน

นโยบายธรรมาภิบาลข้อมูลของกรมราชทัณฑ์ พ.ศ. 2568

โดยที่รัฐธรรมนูญแห่งราชอาณาจักรไทยบัญญัติให้มีการปฏิรูปประเทศด้านการบริหารราชการแผ่นดิน โดยให้นำเทคโนโลยีที่เหมาะสมมาประยุกต์ใช้ในการบริหารราชการและการจัดทำบริการสาธารณะ รวมถึงให้มีการบูรณาการฐานข้อมูลของหน่วยงานของรัฐ เพื่ออำนวยความสะดวกแก่ประชาชนและยกระดับการบริหารงานและการให้บริการภาครัฐให้อยู่ในระบบดิจิทัล

กรมราชทัณฑ์ ในฐานะหน่วยงานของรัฐที่มีภารกิจเกี่ยวข้องกับการควบคุม พัฒนาพฤตินิสัย และการฟื้นฟูผู้ต้องขัง เพื่อคืนคนดีสู่สังคม จำเป็นต้องมีระบบบริหารจัดการและกระบวนการควบคุมข้อมูลที่เหมาะสม โดยมีมาตรการควบคุมการเข้าถึงข้อมูล การพัฒนาคุณภาพของข้อมูล และหลักประกันในการคุ้มครองข้อมูลให้มีความมั่นคงปลอดภัย รวมถึงคุ้มครองข้อมูลส่วนบุคคลของผู้ต้องขัง เจ้าหน้าที่ และประชาชนที่เกี่ยวข้อง ทั้งนี้ เพื่อให้การบริหารจัดการข้อมูลของกรมราชทัณฑ์เป็นไปตามหลักธรรมาภิบาลข้อมูลภาครัฐ ตามมาตรา 8 แห่งพระราชบัญญัติการบริหารงานและการให้บริการภาครัฐผ่านระบบดิจิทัล พ.ศ. 2562 จึงสมควรกำหนดนโยบายธรรมาภิบาลข้อมูลของกรมราชทัณฑ์ ดังต่อไปนี้

วัตถุประสงค์

1. เพื่อให้กรมราชทัณฑ์มีนโยบายธรรมาภิบาลข้อมูลในการบริหารจัดการข้อมูลที่สอดคล้องกับพระราชบัญญัติที่เกี่ยวข้อง ได้แก่
    - พระราชบัญญัติการบริหารงานและการให้บริการภาครัฐผ่านระบบดิจิทัล
    - พระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ. 2540
    - พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562
    - กรอบธรรมาภิบาลข้อมูลภาครัฐ ของสำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน)
2. เพื่อกำหนดขอบเขตของการบริหารจัดการข้อมูล ตั้งแต่การเก็บรวบรวม การใช้ การประมวลผล และการเปิดเผยข้อมูลของกรมราชทัณฑ์
3. เพื่อใช้เป็นแนวทางในการพัฒนาแนวปฏิบัติธรรมาภิบาลข้อมูล โดยยึดหลักคุณภาพ ความมั่นคงปลอดภัย และมาตรฐานสากล

ขอบเขต

นโยบายฉบับนี้มีผลบังคับใช้กับบุคลากรภายในและบุคคลภายนอกที่เกี่ยวข้องกับการจัดการข้อมูลของกรมราชทัณฑ์ เช่น เจ้าหน้าที่ราชทัณฑ์ คณะกรรมการ ผู้รับจ้าง นิสิตนักศึกษาฝึกงาน เป็นต้น ทั้งนี้ ผู้เกี่ยวข้องต้องปฏิบัติตามนโยบายและแนวปฏิบัติธรรมาภิบาลข้อมูลอย่างเคร่งครัด

ข้อ 1 โครงสร้างธรรมาภิบาลข้อมูล (Data Governance Structure)

บทบาท	ผู้รับผิดชอบ	หน้าที่
ผู้ดูแลข้อมูลทางเทคนิค (Data Custodian)	กรมราชทัณฑ์	กำหนดนโยบายการบริหารจัดการข้อมูลให้เป็นไปตามหลักธรรมาภิบาล
ผู้บริหารข้อมูลระดับสูง (Chief Data Officer)	อธิบดีกรมราชทัณฑ์ (CEO) หรือ ผู้บริหารเทคโนโลยีสารสนเทศระดับสูง (CIO)	กำกับดูแลธรรมาภิบาลข้อมูลทั้งหมดของกรม
คณะกรรมการธรรมาภิบาลข้อมูล	ตามคำสั่งกรมราชทัณฑ์	ให้คำปรึกษาและเสนอแนะด้านการบริหารข้อมูล
ผู้บริหารข้อมูล (Data Executive)	ผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศ	ดูแลการจัดการข้อมูลแบบครบวงจร
เจ้าของข้อมูล (Data Owner)	ผู้อำนวยการ สำนัก/กอง/กลุ่ม/ศูนย์	ตรวจสอบ อนุมัติ และจัดชั้นความลับของข้อมูล
ทีมบริกรข้อมูล (Data Stewards)	คณะทำงานกำกับดูแลข้อมูล	พัฒนามาตรฐาน ตรวจสอบคุณภาพข้อมูล
ผู้สร้างข้อมูล (Data Creators)	เจ้าหน้าที่, ผู้ต้องขัง, เจ้าหน้าที่บันทึก	บันทึก แก้ไข ลบข้อมูลให้สอดคล้องตามมาตรฐาน
ผู้เชี่ยวชาญข้อมูล (Data Specialists)	ผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศ	ให้การสนับสนุนด้านเทคนิคและธุรกิจ
ผู้ใช้ข้อมูล (Data Users)	เจ้าหน้าที่และบุคคลภายนอกที่ได้รับอนุญาต	ใช้ข้อมูลอย่างปลอดภัย และรายงานปัญหา

ข้อ 2 นโยบายการเข้าถึงข้อมูล (Data Access Policy)

1. การบริหารจัดการข้อมูลของกรมราชทัณฑ์ ตั้งแต่การเก็บรวบรวม การใช้ การประมวลผล รวมถึงการเปิดเผยข้อมูล ต้องมีการกำหนดสิทธิ หน้าที่ และความรับผิดชอบ เพื่อควบคุมให้อยู่ในขอบเขตที่สามารถกระทำได้โดยไม่ขัดต่อกฎหมาย ระเบียบ ความลับของทางราชการ และความเป็นส่วนบุคคล และต้องมีการกำหนดกระบวนการความมั่นคงปลอดภัยข้อมูลอย่างเคร่งครัด เพื่อรักษาคุณภาพ ความปลอดภัย และความสมบูรณ์ของข้อมูล

2. ผู้ใช้ข้อมูล และทุกคนที่เกี่ยวข้องกับวงจรชีวิตข้อมูลของกรมกรมราชทัณฑ์ มีสิทธิในการเข้าถึงข้อมูล และระบบสารสนเทศของกรมราชทัณฑ์ เพื่อการปฏิบัติงานเฉพาะในส่วนที่ได้รับอนุญาตตามการกำหนดสิทธิในแนวปฏิบัติธรรมาภิบาลข้อมูลของกรมราชทัณฑ์เท่านั้น เช่น ข้อมูลเปิดเผยต่อสาธารณะสามารถเข้าถึงได้โดยสาธารณะ และข้อมูลที่มีชั้นความลับจะสามารถเข้าถึงได้เฉพาะผู้ที่ได้รับสิทธิการเข้าถึงโดยเจ้าของข้อมูลเท่านั้น เป็นต้น

3. ในกรณีที่ผู้ใช้ข้อมูลถูกปฏิเสธการเข้าถึงข้อมูล สามารถยื่นคำร้องกับคณะกรรมการธรรมาภิบาลข้อมูลเพื่อพิจารณาการให้สิทธิ

4. การขอสิทธิเข้าถึงข้อมูลสำหรับประชาชนทั่วไปให้เป็นไปตามพระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ. 2540

ข้อ 3 นโยบายการใช้ข้อมูล (Data Usage Policy)

1. การรวบรวมข้อมูล ที่รวบรวมจากทั้งหน่วยงานภายในและหน่วยงานภายนอก ทั้งที่รวบรวมมาโดยอัตโนมัติจากระบบหรืออุปกรณ์ต่าง ๆ หรือข้อมูลที่เกิดขึ้นจากการป้อนข้อมูลหรือโต้ตอบกับผู้ใช้งานต้องได้รับการบริหารจัดการอย่างถูกต้อง เหมาะสม และสอดคล้องกับวัตถุประสงค์ในการบริหารจัดการข้อมูลของหน่วยงาน สำหรับข้อมูลที่มาจากภายนอก จะต้องมีการตรวจสอบคุณภาพและความน่าเชื่อถือก่อนนำข้อมูลภายนอกมาเชื่อมโยงกับระบบฐานข้อมูลของกรมราชทัณฑ์

2. การจัดเก็บข้อมูล ต้องมีการกำหนดสภาพแวดล้อมของการจัดเก็บข้อมูลที่มีความปลอดภัยทั้งในด้านสถานที่และด้านเทคโนโลยีที่ใช้ในการจัดเก็บข้อมูล ทั้งนี้ ไม่ว่าข้อมูลนั้นจะอยู่ในรูปของข้อมูลอิเล็กทรอนิกส์ หรือรูปแบบอื่นใด โดยต้องมีการกำกับดูแลเทคโนโลยีสารสนเทศให้มีประสิทธิภาพ มีความน่าเชื่อถือ และให้มีการดำเนินงานและการให้บริการที่ได้มาตรฐานสากล

3. การนำข้อมูลไปใช้หรือประมวลผล ต้องมีการควบคุมให้อยู่ในขอบเขตที่สามารถกระทำได้โดยไม่ขัดต่อกฎหมาย ระเบียบ ความลับของทางราชการ และความเป็นส่วนบุคคล โดยสามารถป้องกันไม่ให้บุคคลที่ไม่มีสิทธิทำการแก้ไข เปลี่ยนแปลง หรือทำลายข้อมูลได้

4. การเปิดเผยและแลกเปลี่ยนข้อมูลต้องอยู่ภายใต้บังคับของกฎหมายที่เกี่ยวข้อง โดยทีมบริกรข้อมูลจะต้องกำหนดมาตรฐานในการเปิดเผยและแลกเปลี่ยนข้อมูลที่มีประสิทธิภาพ สามารถนำไปใช้ได้จริง เช่น มีการแลกเปลี่ยนข้อมูลในรูปแบบของ Application Programming Interfaces (API)

มี Framework ที่กำหนดกระบวนการการบูรณาการข้อมูล และต้องมีการกำหนดมาตรการรักษาความมั่นคงปลอดภัยในการแลกเปลี่ยนข้อมูล โดยควรกำหนดหัวข้อต่อไปนี้

(1) ประเภทของข้อมูลที่สามารถแลกเปลี่ยนได้

(2) วิธีการแลกเปลี่ยนข้อมูล

(3) วิธีการป้องกันข้อมูลที่มีความสำคัญ

(4) ระบุผู้รับผิดชอบหรือขอบเขตความรับผิดชอบหากข้อมูลสูญหาย หรือถูกทำลายระหว่างการแลกเปลี่ยน

5. การทำลายข้อมูล ต้องมีการทบทวนข้อมูลที่จัดเก็บอย่างสม่ำเสมอ ทั้งที่อยู่ในรูปแบบอิเล็กทรอนิกส์ และรูปแบบกระดาษ เมื่อข้อมูลไม่มีความจำเป็นต้องใช้งานแล้ว หรือพ้นระยะเวลาการจัดเก็บรักษา ให้พิจารณาลบหรือทำลายข้อมูลดังกล่าว โดยข้อมูลจะถูกเก็บและทำลายด้วยวิธีการที่ถูกต้องตรงตามนโยบายในการจัดเก็บข้อมูลของกรมราชทัณฑ์ และตรงตามกระบวนการของกฎหมาย

6. การดำเนินการด้านความมั่นคงปลอดภัยของข้อมูล ต้องจัดให้มีมาตรการการรักษาความมั่นคงปลอดภัยและการรักษาความเป็นส่วนบุคคล โดยต้องควบคุมและจัดการข้อมูลตามวงจรชีวิตของข้อมูล รวมถึงต้องมีการประเมินด้านความมั่นคงปลอดภัยของข้อมูลตามประเภทของข้อมูล ทั้งนี้ อย่างน้อยปีละ 1 ครั้ง หรือเมื่อมีเหตุการณ์ที่สำคัญ โดยให้สอดคล้องกับมาตรการรักษาความมั่นคงปลอดภัยของผู้ควบคุมข้อมูลส่วนบุคคล ตามประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล

ข้อ 4 นโยบายบูรณภาพของข้อมูล (Data Integrity and Integration Policy)

1. ต้องมีกระบวนการรักษาคุณภาพและความสมบูรณ์ของข้อมูล (Data Integrity) เพื่อให้ข้อมูลมีความถูกต้องและน่าเชื่อถืออยู่เสมอ

2. ข้อมูลจะต้องมีมีความเป็นปัจจุบันในทุกขั้นตอนของการดำเนินการ และสามารถตรวจสอบได้

3. ก่อนที่ข้อมูลจะถูกใช้งานหรือเผยแพร่สู่ภายนอก ข้อมูลนั้นจะต้องมีการตรวจสอบกับบริกรข้อมูล ทั้งนี้ เพื่อรักษาไว้ซึ่งคุณภาพ ความปลอดภัย และความสมบูรณ์ของข้อมูล

ทั้งนี้ เพื่อให้นโยบายธรรมาภิบาลข้อมูลมีความทันสมัย สอดคล้องกับสถานการณ์ปัจจุบัน คณะกรรมการและทีมบริกรข้อมูล ต้องมีการทบทวนนโยบายอย่างน้อยปีละ 1 ครั้ง และทุกครั้งที่มีการเปลี่ยนแปลงที่สำคัญ