PTG Energy Group

เอกสารสนับสนุน

เรื่อง

นโยบายการกำกับดูแลข้อมูล
(Data Governance Policy)

ประวัติการแก้ไข

00	16/10/68	จัดทำครั้งแรก
แก้ไขครั้งที่	**วันที่บังคับใช้**	**รายละเอียดการแก้ไข**

1. วัตถุประสงค์

ข้อมูลถือเป็นทรัพย์สินที่สำคัญของกลุ่มบริษัท การมีข้อมูลที่มีคุณภาพและน่าเชื่อถือนำมาซึ่งการใช้ประโยชน์จากข้อมูลในการสร้างโอกาสทางธุรกิจใหม่ๆ การเพิ่มประสิทธิภาพในการปฏิบัติงานและการตัดสินใจให้ดียิ่งขึ้นได้ จึงจัดทำนโยบายการกำกับดูแลข้อมูลให้สอดคล้องและเป็นไปตามกรอบการกำกับดูแลกิจการ กฎหมายและกฎเกณฑ์ที่เกี่ยวข้องกับการกำกับดูแลข้อมูล รวมถึงมาตรฐานที่ยอมรับและเชื่อถือ เพื่อใช้เป็นมาตรฐานเดียวกันทั้งองค์กร

2. ขอบเขตของนโยบาย

2.1 การบังคับใช้

นโยบายนี้มีผลบังคับใช้กับพนักงานทุกระดับ ผู้บริหาร คู่ค้าและหน่วยงานต่างๆ ของบริษัท พีทีจี เอ็นเนอยี จำกัด (มหาชน) และบุคคลภายนอกที่เกี่ยวข้องกับระบบสารสนเทศ หรือสามารถเข้าถึงข้อมูลที่สำคัญของบริษัท

2.2 วันที่มีผลใช้บังคับ

นโยบายนี้มีผลใช้บังคับกับกิจกรรมทั้งหมดของกลุ่มบริษัท นับตั้งแต่วันที่ได้รับการอนุมัติจากคณะกรรมการบริษัท

2.3 การทบทวนนโยบาย

นโยบายนี้จะได้รับการทบทวนเป็นประจำทุกปี หรือเมื่อมีการเปลี่ยนแปลงอย่างมีนัยสำคัญ หรือมีการเปลี่ยนแปลงกฎหมายที่กระทบสาระสำคัญของนโยบาย

3. คำจำกัดความ

กลุ่มบริษัท	หมายถึง บริษัท พีทีจี เอ็นเนอยี จำกัด (มหาชน) และบริษัทย่อย หรือนิติบุคคลใด ๆ ที่จะดำเนินการจดทะเบียนจัดตั้งให้เป็นบริษัทย่อย หรือบริษัทร่วมของ บริษัท พีทีจี เอ็นเนอยี จำกัด (มหาชน) เพิ่มเติมต่อไปในภายหน้า
พนักงาน	หมายถึง พนักงานบริษัท พนักงานสัญญาจ้าง และพนักงานของหน่วยงานภายนอกที่เข้ามาปฏิบัติงานที่เกี่ยวข้องกับข้อมูลหรือระบบข้อมูลของบริษัท
การกำกับดูแลข้อมูล	หมายถึง แนวทางและนโยบาย หรือธรรมาภิบาลข้อมูลในการกำกับดูแลข้อมูลตลอดวงจรชีวิตของข้อมูล (Data Life Cycle) ตั้งแต่การรวบรวม จัดเก็บ ประมวลผล ไปจนถึงการทำลายข้อมูล โดยมีจุดประสงค์เพื่อกำหนดหน้าที่ ความรับผิดชอบ และมาตรฐานในการดูแลจัดการข้อมูลให้เป็นระเบียบ ชัดเจน และมีคุณภาพ
วงจรชีวิตของข้อมูล (Data Life Cycle)	หมายถึง ลำดับขั้นตอนของข้อมูลโดยเริ่มตั้งแต่ การเกิดขึ้นของข้อมูล วิธีเก็บข้อมูล การนำไปใช้ การแชร์ข้อมูล การจัดเก็บถาวร และการทำลายข้อมูล
ทะเบียนข้อมูล	หมายถึง รายการของชุดข้อมูล ซึ่งสามารถจัดเตรียมได้ในรูปแบบของตาราง รายชื่อชุดข้อมูล รายงาน หรือแอปพลิเคชัน บัญชีข้อมูลถูกใช้เพื่อความสะดวกในการค้นหาชุดข้อมูล (Datasets) หรือคำอธิบายชุดข้อมูล (Metadata)

4. หลักการและแนวปฏิบัติ

กลุ่มบริษัท กำหนดหลักการและแนวทางไว้ในนโยบายฉบับนี้ เพื่อให้การบริหารจัดการข้อมูลของกลุ่มบริษัท มีประสิทธิภาพและเกิดประสิทธิผล สอดคล้องกับข้อกำหนดของกฎหมาย และมาตรฐานด้านความมั่นคงปลอดภัยของข้อมูลและมาตรฐานการปฏิบัติงานที่เกี่ยวข้อง ดังต่อไปนี้

4.1 การกำกับดูแลข้อมูลและการบริหารจัดการข้อมูลตามวงจรชีวิตข้อมูล (Data Life Cycle) โดยกำหนดโครงสร้างการกำกับดูแลข้อมูลอย่างเหมาะสม มีระบบการตรวจสอบและถ่วงดุล (Checks and Balances) อย่างโปร่งใส ตามหลักแนวป้องกัน 3 ชั้น (Three Lines of Defense) ซึ่งประกอบด้วย

4.1.1 คณะทำงานกำกับดูแลข้อมูล (Data Governance Working Team) ทำหน้าที่กำกับดูแลและกำหนดแนวนโยบายและแนวทางปฏิบัติให้สอดคล้องกับมาตรฐานของการบริหารจัดการข้อมูลตามวงจรชีวิตของข้อมูลและมาตรฐานการรักษาความมั่นคงปลอดภัยของระบบข้อมูล และส่งเสริม สนับสนุน ให้คำปรึกษาและคำแนะนำแก่หน่วยงานต่างๆ ในการปฏิบัติงานด้านการกำกับดูแลและบริหารจัดการข้อมูลให้เป็นไปตามกฎหมายและมาตรฐานที่เกี่ยวข้อง

4.1.2 ผู้บริหารระดับสูงด้านข้อมูล เพื่อพิจารณากลั่นกรองและบริหารจัดการข้อมูลของแต่ละหน่วยงานให้ครบทั้งวงจรชีวิตของข้อมูล (Data Life Cycle) ซึ่งอาจมีการแต่งตั้งหรือมอบหมายผู้บริหารด้านข้อมูลระดับส่วนงานเพื่อช่วยควบคุมดูแลและบริหารจัดการข้อมูลของส่วนงาน

4.1.3 ผู้ปฏิบัติงานที่เกี่ยวข้องกับข้อมูล ไม่ว่าจะอยู่ในสถานะเจ้าของข้อมูล (Data Owner) ผู้ใช้ข้อมูล หรือผู้ดูแลระบบจัดเก็บข้อมูล (System Admin) เพื่อทำหน้าที่ให้ชัดเจนตามขอบเขตสิทธิและหน้าที่ที่กลุ่มบริษัท กำหนด

4.1.4 หน่วยงานบริหารความเสี่ยง เป็นหน่วยงาน 2nd Line ทำหน้าที่กำหนดความเสี่ยงและมาตรการบริหารจัดการความเสี่ยงให้ครอบคลุมความเสี่ยงด้านข้อมูลอย่างเหมาะสม

4.1.5 หน่วยงานกำกับดูแลการปฏิบัติตามกฎหมาย เป็นหน่วยงาน 2nd Line ทำหน้าที่สอบทานการปฏิบัติงานเพื่อให้มั่นใจว่าการบริหารจัดการข้อมูลสอดคล้องกับนโยบาย ข้อกฎหมายและระเบียบปฏิบัติที่เกี่ยวข้อง

4.1.6 สำนักคุ้มครองข้อมูลส่วนบุคคล (DPO) ทำหน้าที่สอบทานการปฏิบัติงานเพื่อให้มั่นใจว่าการบริหารจัดการข้อมูลส่วนบุคคลของบริษัท สอดคล้องกับนโยบาย ข้อกฎหมายและระเบียบปฏิบัติที่เกี่ยวข้อง

4.1.7 หน่วยงานตรวจสอบภายใน เป็นหน่วยงาน 3rd Line ทำหน้าที่ตรวจสอบการปฏิบัติตามนโยบายและมาตรฐาน เพื่อให้มั่นใจว่าการบริหารจัดการข้อมูลขององค์กรเป็นไปตามนโยบายและมาตรฐานที่องค์กรกำหนดไว้อย่างถูกต้อง การตรวจสอบครอบคลุมตั้งแต่การสร้าง การจัดเก็บ การประมวลผล การใช้ ไปจนถึงการทำลายข้อมูล

4.2 กำกับดูแลข้อมูลโดยยึดมั่นและปฏิบัติตามนโยบายและระเบียบปฏิบัติว่าด้วยความมั่นคงปลอดภัยของข้อมูล (Data Security) การปกป้องความเป็นส่วนตัวของข้อมูล (Data Privacy) และการรักษาคุณภาพข้อมูลให้มีความถูกต้อง ครบถ้วน และเป็นปัจจุบัน (Data Quality)

4.3 กำกับดูแลข้อมูลโดยคำนึงถึงประโยชน์ ความคุ้มค่า การรักษาความลับความปลอดภัย และความเสี่ยงที่ยอมรับได้ของกลุ่มบริษัท เป็นสำคัญ โดยการจะครอบคลุมตั้งแต่การสร้าง (Create) การจัดเก็บ (Store) การใช้ (Use) การเปิดเผย (Public) การจัดการกับข้อมูลเมื่อสิ้นสุดการใช้งานตามวงจรชีวิตของข้อมูล

4.4 การบริหารจัดการข้อมูลที่ใช้ร่วมกัน จัดทำบัญชีข้อมูลหรือจัดทำบันทึกทะเบียนข้อมูลให้ครบถ้วน รวมถึงมีการประเมินคุณภาพของข้อมูล (Data Quality Assessment) และประเมินความมั่นคงปลอดภัยของข้อมูล (Data Security Assessment) อย่างสม่ำเสมอและต่อเนื่อง

4.5 การจัดเก็บและดำเนินการกับข้อมูลที่ได้มาให้สอดคล้องกับความต้องการและวัตถุประสงค์ในการดำเนินงานตามที่กฎหมายกำหนด และมีการจัดชั้นความลับของข้อมูลให้สอดคล้องกับ

นโยบายการรักษาความมั่นคงปลอดภัยด้านสารสนเทศและมีการจัดการกับข้อมูลตามชั้นความลับที่กำหนด

4.6 กำหนดให้มีการแลกเปลี่ยนข้อมูล การเปิดเผยข้อมูล และการกำหนดสิทธิ์การเข้าถึงข้อมูลที่เหมาะสมคำนึงถึงความมั่นคงปลอดภัยและป้องกันการรั่วไหลของข้อมูลเป็นสำคัญ มีการจัดทำข้อตกลงที่ชัดเจนในการแลกเปลี่ยนข้อมูล หรือใช้ข้อมูลเพื่อปฏิบัติงาน และในการเปิดเผยข้อมูลจะต้องได้รับความยินยอมจากเจ้าของข้อมูล หรือสอดคล้องกับข้อตกลงหรือสัญญา เว้นแต่จะมีกฎหมายบัญญัติให้กระทำได้ รวมถึงมีการกำหนดสิทธิ์เข้าถึงข้อมูลอย่างเหมาะสม และมีเครื่องมือในการตรวจสอบการเข้าถึงข้อมูลที่ผิดปกติ

4.7 ให้ความสำคัญกับการคุ้มครองข้อมูลส่วนบุคคล ทั้งการเก็บ รวบรวม ประมวลผลอย่างมีความรับผิดชอบและปฏิบัติตามนโยบายและกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล

4.8 มีการติดตามและจัดการปัญหาข้อร้องเรียนที่เกี่ยวข้องกับข้อมูลด้วยกระบวนการที่เหมาะสมและเป็นธรรมต่อผู้มีส่วนได้เสีย

4.9 มีการสื่อสารสร้างความตระหนักรู้ด้านการกำกับดูแลข้อมูลให้กับพนักงานทุกระดับ รวมถึงมีกระบวนการให้ผู้ให้บริการภายนอกรับทราบและลงนามยอมรับเงื่อนไขการว่าจ้างที่ครอบคลุมการรักษาความมั่นคงปลอดภัยของข้อมูล และการรักษาข้อมูลความลับของกลุ่มบริษัท และข้อมูลส่วนบุคคลของลูกค้า

4.10 ในการนำข้อมูลมาวิเคราะห์และใช้ประโยชน์เพื่อการกำหนดนโยบาย กลยุทธ์ ออกแบบผลิตภัณฑ์และบริการให้ตรงตามความต้องการของลูกค้าและผู้มีส่วนได้ส่วนเสีย หรือเพื่อสร้างมูลค่าเพิ่มให้กับกลุ่มบริษัท กลุ่มบริษัท คำนึงถึงการรักษาความลับของข้อมูล การคุ้มครองข้อมูลส่วนบุคคล รวมถึงหลักการบริหารจัดการข้อมูล รวมถึงหลักธรรมาภิบาลปัญญาประดิษฐ์ (AI Governance)

4.11 มีกระบวนการและขั้นตอนการรายงานผลการดำเนินงานตามนโยบายการกำกับดูแลข้อมูลให้คณะกรรมการกำกับดูแลกิจการและความยั่งยืน คณะกรรมการตรวจสอบ และคณะกรรมการบริษัทอย่างสม่ำเสมอ

5. การฝ่าฝืนหรือไม่ปฏิบัติตาม

กรณีฝ่าฝืนหรือจงใจไม่ปฏิบัติตามนโยบายฉบับนี้ อาจต้องรับผิดตามข้อบังคับการทำงานของกลุ่มบริษัทหรือรับโทษทางวินัย หรือถูกพิจารณาดำเนินการทางกฎหมาย หากก่อให้เกิดความเสียหายต่อองค์กร ลูกค้า หรือผู้มีส่วนได้ส่วนเสียอื่นๆ