ประกาศนโยบายธรรมาภิบาลข้อมูล

(Data Governance Policy)

1. หลักการ

กลุ่มบริษัทพาราวินเซอร์ มีข้อมูลจัดเป็นหนึ่งในทรัพย์สินที่สำคัญ และเป็นกลไกในการขับเคลื่อนการดำเนินงานของ กลุ่มบริษัทพาราวินเซอร์ ทั้งในด้านการจัดเก็บข้อมูล การเปิดเผยข้อมูล ความมั่นคงปลอดภัยของข้อมูล และด้านคุณภาพของข้อมูล เพื่อให้การนำข้อมูลไปใช้ก่อให้เกิดประโยชน์อย่างเต็มที่และมีประสิทธิภาพ สามารถนำไปใช้และบริหารจัดการข้อมูลของบริษัททุกขั้นตอนอย่างเป็นระบบ มีความชัดเจนและเป็นไปตามกฎหมาย

2. วัตถุประสงค์

1. เพื่อให้ กลุ่มบริษัทพาราวินเซอร์ สามารถดำเนินการด้านข้อมูล รวมถึงติดตามการบริหารจัดการข้อมูลให้มีความโปร่งใสตรวจสอบได้ ส่งผลต่อคุณภาพของข้อมูล ความมั่นคงปลอดภัยของข้อมูล และบูรณาการข้อมูลหรือวงจรชีวิตของข้อมูลทำให้ข้อมูลมีความถูกต้อง ความครบถ้วน ความต้องกัน ความเป็นปัจจุบัน ความต้องการของผู้ใช้ และความพร้อมใช้

2. เพื่อให้การส่งมอบคุณค่าของข้อมูลเป็นไปโดยสอดคล้องกับยุทธศาสตร์ กลุ่มบริษัทพาราวินเซอร์

3. เพื่อให้ กลุ่มบริษัทพาราวินเซอร์ ได้รับข้อมูลที่มีคุณภาพที่ดียิ่งขึ้น (Data Quality) สามารถใช้ข้อมูลเพื่อบรรลุเป้าประสงค์ทางยุทธศาสตร์ได้อย่างมีประสิทธิภาพ

3. คำนิยาม

“กลุ่มบริษัทพาราวินเซอร์” ประกอบด้วยจำนวน 18 บริษัท (ตามเอกสารแนบ)

“ผู้จัดการ” หมายความว่า ผู้จัดการซึ่งได้รับมอบอำนาจจากผู้บริหารสูงสุด หรือกรรมการผู้มีอำนาจให้ดำเนินการเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลตามประกาศนโยบายธรรมาภิบาลข้อมูล

“พนักงาน” หมายความว่า พนักงาน ลูกจ้าง ผู้รับจ้าง ที่ปรึกษา นักศึกษาฝึกงาน หรือผู้ที่กลุ่มบริษัทพาราวินเซอร์จ้างไว้ปฏิบัติงาน ทั้งในลักษณะประจำ หรือมีกำหนดระยะเวลา หรือเป็นครั้งคราว และรับเงินเดือน ค่าตอบแทน หรือเบี้ยเลี้ยง ตามตำแหน่งและขั้นที่บรรจุ และรวมถึงตำแหน่งผู้จัดการ

“ข้อมูล” หมายความว่า สิ่งที่สื่อความหมายให้รู้เรื่องราวข้อเท็จจริง ข้อมูลหรือสิ่งใดๆ ไม่ว่าการสื่อความหมายนั้นจะทำได้โดยสภาพของสิ่งนั้นเองหรือโดยผ่านวิธีการใดๆ และไม่ว่าจะจัดทำไว้ในรูปแบบของเอกสาร แฟ้ม รายงาน หนังสือ แผนผัง แผนที่ ภาพวาด ภาพถ่าย ฟิล์ม การบันทึกภาพหรือเสียงการบันทึกโดยเครื่องคอมพิวเตอร์หรือวิธีอื่นใดที่ทำให้สิ่งที่บันทึกไว้ปรากฏเป็นทรัพย์สินชนิดหนึ่งที่มีมูลค่าและความสำคัญแก่กลุ่มบริษัท

“ข้อมูลส่วนบุคคล” หมายความว่า ข้อมูลเกี่ยวกับบุคคลซึ่งทำให้สามารถระบุตัวบุคคลนั้นได้ ไม่ว่าทางตรงหรือทางอ้อม แต่ไม่รวมถึงข้อมูลของผู้ถึงแก่กรรม

“เจ้าของข้อมูล” (Data Owner) หมายความว่า บุคคลที่ทำหน้าที่ตรวจสอบดูแลข้อมูลโดยตรง สร้างความมั่นใจได้ว่าการบริหารจัดการข้อมูลสอดคล้องกับนโยบาย มาตรฐาน กฎระเบียบ หรือกฎหมาย เจ้าของข้อมูลทำการทบทวนและอนุมัติการดำเนินการต่าง ๆ ที่เกี่ยวข้องกับข้อมูล

“หน่วยงาน” หมายความว่า สายงาน กลุ่มงาน ฝ่ายงาน หรือ สำนักของกลุ่มบริษัท

“ธรรมาภิบาลข้อมูล” หมายความว่า การกำหนดสิทธิ หน้าที่และความรับผิดชอบของผู้มีส่วนได้เสียในการบริหารจัดการข้อมูลทุกขั้นตอน เพื่อให้การได้มาและการนำไปใช้ข้อมูลของหน่วยงานถูกต้อง ครบถ้วน เป็นปัจจุบัน รักษาความเป็นส่วนบุคคล และสามารถเชื่อมโยงกันได้อย่างมีประสิทธิภาพ และมั่นคงปลอดภัย

“ระบบเทคโนโลยีสารสนเทศ” หมายความว่า ข้อมูลของกลุ่มบริษัทที่พร้อมสำหรับการใช้งาน หรือได้รับการรวบรวมไว้สำหรับใช้งาน ได้แก่ แบบฟอร์มและเอกสารสายงานสารสนเทศ ฐานข้อมูล โปรแกรมประยุกต์ต่างๆ เป็นต้น

“เมทาดาตา” (Metadata) หมายความว่า คำอธิบายชุดข้อมูล ซึ่งเป็นข้อมูลที่ใช้กำกับและอธิบายข้อมูลหลักหรือกลุ่มของข้อมูลอื่นๆ ที่เกี่ยวข้องทั้งกระบวนการเชิงธุรกิจและเชิงเทคโนโลยีสารสนเทศ

“ฐานข้อมูล” หมายความว่า กลุ่มข้อมูลที่มีความสัมพันธ์กันได้ถูกรวบรวมเข้าไว้ด้วยกัน ซึ่งสนับสนุนกิจกรรมของกลุ่มบริษัท

“คลังข้อมูล” หมายความว่า เป็นข้อมูลที่ได้จากการเชื่อมโยงข้อมูล (Data Integration) ซึ่งเกิดจากการรวบรวมข้อมูลจากแหล่งข้อมูลต่าง ๆ ที่มีหลากหลายรูปแบบมาเก็บในคลังข้อมูลต่างๆของกลุ่มบริษัท

“วงจรชีวิตข้อมูล” หมายความว่า ลำดับขั้นตอนของข้อมูลตั้งแต่เริ่มสร้างข้อมูลไปจนถึงการทำลายข้อมูล ประกอบด้วย 6 ขั้นตอน คือ การสร้างข้อมูล การจัดเก็บข้อมูล การใช้ข้อมูล การเผยแพร่ข้อมูล การจัดเก็บข้อมูลถาวร การทำลายข้อมูล

4. นโยบายธรรมาภิบาลข้อมูล

การกำหนดนโยบายธรรมาภิบาลข้อมูลจัดเป็นหนึ่งในพื้นฐานของธรรมาภิบาลข้อมูล เพื่อให้ครอบคลุมระบบบริหารและกระบวนการจัดการข้อมูลหรือวงจรชีวิตของข้อมูล ทั้งนี้การจัดทำนโยบายธรรมาภิบาลข้อมูลประกอบด้วย รายละเอียดทั่วไปที่เกี่ยวข้องกับข้อมูล การสร้างข้อมูล การจัดเก็บข้อมูลและทำลายข้อมูล การประมวลผลข้อมูลและการใช้ข้อมูล การแลกเปลี่ยนและการเชื่อมโยงข้อมูล การเปิดเผยข้อมูล การวัดการดำเนินการและความสำเร็จของธรรมาภิบาลข้อมูล

5. ทั่วไป

เพื่อกำหนดรายละเอียดทั่วไปที่เกี่ยวข้องกับข้อมูล เช่น โครงสร้างที่เกี่ยวข้อง หน้าที่ความรับผิดชอบ โดยมีรายละเอียด ดังนี้

5.1 กำหนดบทบาทและความรับผิดชอบที่ประกอบกันเป็นโครงสร้างธรรมาภิบาลข้อมูล โดยต้องได้รับการมอบอำนาจและการอนุมัติจากผู้จัดการ

5.2 กำหนดกลุ่มบุคคลหรือบุคคลภายในกลุ่มบริษัท เพื่อเป็นเจ้าของข้อมูลในการบริหารจัดการข้อมูลของหน่วยงานเพราะหน่วยงานถือเป็นเจ้าของข้อมูลทุกประเภทที่เกิดจากการดำเนินงานภายในหน่วยงานนั้นๆ

5.3 กำหนดขอบเขตข้อมูลที่นโยบายธรรมาภิบาลข้อมูลครอบคลุม เช่น

- ข้อมูลที่มีโครงสร้าง (ฐานข้อมูล และ Comma Separated Value (CSV))
- ข้อมูลกึ่งโครงสร้าง (Extensible Markup Language (XML) และ JavaScript Object Notation (JSON))
- ข้อมูลที่ไม่มีโครงสร้าง (เอกสาร เสียง ภาพ และภาพเคลื่อนไหว)

5.4 กำหนดมาตรการการรักษาความปลอดภัยของข้อมูล เพื่อป้องกันการเข้าถึง การสูญหาย การทำลาย หรือการเปลี่ยนแปลงข้อมูลโดยไม่ได้รับการอนุญาต

5.5 นำระบบเทคโนโลยีสารสนเทศหรือระบบอัตโนมัติมาใช้ในการจัดทำเมทาดาตา

5.6 ตรวจสอบความสอดคล้องกันระหว่างนโยบายธรรมภิบาลข้อมูลกับการดำเนินการใด ๆ ของผู้มีส่วนได้เสียอย่างน้อยปีละ 1 ครั้ง

5.7 ทบทวนนโยบายธรรมภิบาลข้อมูล อย่างน้อยปีละ 1 ครั้ง และให้ดำเนินการปรับปรุงอย่างต่อเนื่อง หากพบว่านโยบายธรรมาภิบาลข้อมูลยังไม่มีประสิทธิภาพเพียงพอ

5.8 สื่อสารและเผยแพร่นโยบายธรรมาภิบาลข้อมูลให้กับผู้ที่เกี่ยวข้องภายในกลุ่มบริษัท

5.9 สนับสนุนให้มีการฝึกอบรมเพื่อสร้างความตระหนักถึงธรรมาภิบาลข้อมูล และการบริหารจัดการข้อมูล โดยให้ครอบคลุมทุกกระบวนการของการบริหารจัดการและระบบบริหารและกระบวนการจัดการข้อมูล (วงจรชีวิตของข้อมูล)

6. บทบาทหน้าที่และความรับผิดชอบ

กลุ่มบริษัทพาราวินเซอร์ กำหนดให้พนักงานหรือหน่วยงานที่เกี่ยวข้องกับข้อมูลส่วนบุคคล ต้องให้ความสำคัญและความรับผิดชอบในการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล ตามประกาศนโยบายธรรมาภิบาลข้อมูลอย่างเคร่งครัด โดยกำหนดให้บุคคลหรือหน่วยงานดังต่อไปนี้ ทำหน้าที่กำกับและตรวจสอบให้การดำเนินงานของบริษัทนั้นถูกต้อง และเป็นไปตามนโยบายและกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคลกำหนด

6.1 ผู้คุ้มครองข้อมูลส่วนบุคคล

6.1.1 จัดให้มีมาตรการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคลที่เหมาะสม และทบทวนมาตรการอย่างสม่ำเสมอเพื่อให้มาตรการดังกล่าวมีประสิทธิภาพ ทันต่อเทคโนโลยีที่เปลี่ยนแปลงไป

6.1.2 กำหนดขอบเขตการจัดการกับข้อมูลส่วนบุคคลให้เป็นไปตามที่กฎหมายกำหนด

6.1.3 จัดให้มีระบบตรวจสอบการจัดการข้อมูลส่วนบุคคลให้เป็นไปตามที่กฎหมายกำหนด

6.1.4 บันทึกรายการเกี่ยวกับข้อมูลส่วนบุคคลตามที่กฎหมายกำหนด

6.1.5 จัดทำข้อตกลงกับผู้ประมวลผลข้อมูลส่วนบุคคล นิติบุคคลหรือบุคคลภายนอกอื่นใด หากมีการเปิดเผยข้อมูลส่วนบุคคลให้แก่ผู้ประมวลผลข้อมูลส่วนบุคคลที่ได้ว่าจ้าง นิติบุคคลหรือบุคคลภายนอกอื่นใด โดยผู้ประมวลผลข้อมูล นิติบุคคล หรือบุคคลภายนอกดังกล่าว ต้องมีมาตรการรักษาความปลอดภัยในการเก็บรวบรวม ใช้ และ/หรือเปิดเผยข้อมูลส่วนบุคคลต้องเป็นไปตามนโยบายฉบับนี้ หรือตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

6.2 ผู้ประมวลผลข้อมูลส่วนบุคคล

6.2.1 ดำเนินการเกี่ยวกับการเก็บรวมรวม ใช้ และ/หรือเปิดเผยข้อมูลส่วนบุคคลตามคำสั่งที่ได้รับจากผู้ควบคุมข้อมูลส่วนบุคคลของบริษัทให้ครบถ้วนและถูกต้องตามที่กฎหมายกำหนด

6.2.2 จัดให้มีมาตรการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคลที่เหมาะสม

6.2.3 จัดทำและเก็บรักษาบันทึกรายการของกิจกรรมการประมวลผลข้อมูลส่วนบุคคลไว้

6.3 เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (Data Protection Officer)

6.3.1 จัดทำและทบทวนนโยบายคุ้มครองข้อมูลส่วนบุคคล รวมถึงแนวปฏิบัติการคุ้มครองข้อมูลส่วนบุคคลของบริษัทให้ครบถ้วนและถูกต้องตามที่กฎหมายกำหนด

6.3.2 ให้คำแนะนำในด้านต่าง ๆ ที่เกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลแก่ผู้บริหาร พนักงาน และคู่ค้าของบริษัท

6.3.3 ตรวจตราการดำเนินงานของผู้ควบคุมข้อมูลส่วนบุคคล และผู้ประมวลผลข้อมูลส่วนบุคคล

6.3.4 กำกับดูแลหน่วยงานต่าง ๆ ของบริษัท และคู่ค้าของบริษัทให้ดำเนินงานตามนโยบายธรรมาภิบาลของบริษัท

6.3.5 รายงานการปฏิบัติงานหน่วยงานต่าง ๆ ของบริษัท และคู่ค้าของบริษัทต่อคณะเจ้าหน้าที่บริหาร

6.3.6 ประสานจัดการเรื่องร้องเรียน หรือการขอใช้สิทธิของเจ้าของข้อมูลส่วนบุคคลที่ได้รับการติดต่อ หรือร้องขอจากเจ้าของข้อมูลส่วนบุคคล

6.3.7 ประสานงาน และให้ความร่วมมือกับสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลในกรณีที่มีปัญหาเกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลของบริษัท บริษัทในเครือ และคู่ค้าของบริษัท

6.3.8 แจ้งต่อสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลทราบถึงเหตุ การละเมิดข้อมูลส่วนบุคคลภายใน 72 ชั่วโมงนับแต่ทราบเหตุเท่าที่จะสามารถทำได้

7. การสร้างข้อมูล

เพื่อกำหนดการสร้างข้อมูลขึ้นมาใหม่ โดยวิธีการบันทึกเข้าไปด้วยบุคคลหรือบันทึกอัตโนมัติด้วยอุปกรณ์อิเล็กทรอนิกส์ เพื่อนำมาจัดเก็บในภายหลัง โดยมีรายละเอียดดังนี้

7.1 กำหนดความสัมพันธ์ระหว่างข้อมูลกับส่วนงาน ข้อมูลกับกระบวนการปฏิบัติงาน และข้อมูลกับระบบงาน

7.2 กำหนดความต้องการของข้อมูล และข้อกำหนดทางธุรกิจโดยเป็นไปตามกฎหมายที่เกี่ยวข้อง

8. การจัดเก็บข้อมูลและทำลายข้อมูล

เพื่อกำหนดการจัดเก็บข้อมูลและทำลายข้อมูลอย่างมีคุณภาพ มีการรักษาความปลอดภัยของข้อมูล โดยมีรายละเอียด ดังนี้

8.1 กำหนดสภาพแวดล้อมของการจัดเก็บข้อมูลที่เอื้อต่อการรักษาความมั่นคงปลอดภัยและคุณภาพของข้อมูล

8.2 กำหนดชั้นความลับของข้อมูล และจัดเก็บให้สอดคล้องกับแนวทางหรือมาตรฐานการ จัดชั้นความลับของข้อมูล (Data Classification Guideline/Standard) ที่กำหนดไว้ เพื่อให้ข้อมูลมีความมั่นคงปลอดภัย และรักษาคุณภาพของข้อมูล

8.3 กำหนดสิทธิ์การเข้าถึงข้อมูล และเครื่องมือที่ใช้ในการเข้าถึงข้อมูล

8.4 จัดเก็บข้อมูลให้สอดคล้องกับความต้องการ และวัตถุประสงค์ในการดำเนินงาน โดยข้อมูลนั้นจะต้องมีความถูกต้อง สมบูรณ์ และเป็นปัจจุบันอยู่เสมอ ทั้งนี้ควรจัดทำเมทาดาตาสำหรับชุดข้อมูลที่มีการจัดเก็บ

8.5 ในกรณีที่มีการร้องขอให้ทำลายข้อมูลส่วนบุคคลจากเจ้าของข้อมูล ผู้ควบคุมหรือหน่วยงานที่จัดเก็บต้องดำเนินการทำลายให้เร็วที่สุด ทั้งนี้ต้องไม่ขัดต่อข้อตกลงระหว่างเจ้าของข้อมูลกับผู้ควบคุม หรือไม่ขัดต่อข้อกฎหมายใด ๆ

8.6 กำหนดแนวทางในการทำลายข้อมูลเมื่อข้อมูลนั้นไม่มีการใช้งานหรือมีการเก็บข้อมูลไว้นานเกินกว่าระยะเวลาที่กำหนด แต่ควรมีการเก็บรักษาเมทาดาตาของข้อมูลที่ทำลายไว้ เพื่อใช้สำหรับการตรวจสอบภายหลัง

8.7 สร้างความรู้ความเข้าใจในการจัดเก็บและทำลายข้อมูลแก่ผู้ที่เกี่ยวข้องภายในกลุ่มบริษัท

9. การประมวลผลข้อมูลและการใช้ข้อมูล

เพื่อกำหนดการประมวลผลข้อมูลและการใช้ข้อมูล ให้ได้ข้อมูลที่มีประสิทธิภาพ ถูกต้อง ตรงตามวัตถุประสงค์ของการใช้ข้อมูลให้เกิดประโยชน์ โดยมีรายละเอียด ดังนี้

9.1 กำหนดแนวปฏิบัติและมาตรฐานของการประมวลผลข้อมูล และทำการสื่อสารให้แก่ผู้ที่เกี่ยวข้องรับทราบ

9.2 การดำเนินการประมวลผลข้อมูลที่เป็นความลับ เช่น ข้อมูลส่วนบุคคล ให้เป็นไปตามขอบเขต เงื่อนไข หรือวัตถุประสงค์ในการยินยอมให้ดำเนินการกับข้อมูลส่วนบุคคลนั้น

9.3 จัดทำเมทาดาตาสำหรับข้อมูลที่จัดเก็บอยู่ในคลังข้อมูล (Data Warehouse)

9.4 ต้องมีการบันทึกประวัติการประมวลผลและการใช้ข้อมูล (Log File) เพื่อให้สามารถตรวจสอบย้อนกลับได้

10. การแลกเปลี่ยนและการเชื่อมโยงข้อมูล

เพื่อกำหนดการแลกเปลี่ยนข้อมูลระหว่างหน่วยงานให้มีความมั่นคงปลอดภัยและข้อมูลมีคุณภาพ สามารถนำไปใช้ประโยชน์ได้อย่างมีประสิทธิภาพ โดยมีรายละเอียด ดังนี้

10.1 กำหนดแนวปฏิบัติในการจัดการเรื่องความมั่นคงปลอดภัย คุณภาพข้อมูล และผู้ประสานงานหรือศูนย์ติดต่อ (Contact Center)

10.2 กำหนดกระบวนการในการแลกเปลี่ยนข้อมูลให้ชัดเจนเริ่มตั้งแต่ขั้นตอนการเตรียมการ ขั้นตอนเริ่มดำเนินการ ขั้นตอนระหว่างดำเนินการ และขั้นตอนสิ้นสุดการดำเนินการ

10.3 กำหนดเมทาดาตาของชุดข้อมูลที่ต้องการแลกเปลี่ยนที่จำเป็นให้ครบถ้วน

10.4 ทำสัญญาอนุญาตหรือข้อตกลงในการแลกเปลี่ยนข้อมูลและการนำข้อมูลไปใช้

10.5 กำหนดเทคโนโลยีและมาตรฐานทางเทคนิคที่ใช้ในการแลกเปลี่ยนข้อมูล

10.6 บันทึกรายละเอียดและจัดเก็บข้อมูลการดำเนินงานที่เกิดขึ้นในแต่ละครั้งที่มีการแลกเปลี่ยนข้อมูล (Log File) ระหว่างหน่วยงาน เพื่อให้สามารถตรวจสอบย้อนกลับได้

10.7 สามารถตรวจสอบได้ว่าการแลกเปลี่ยนข้อมูลได้ดำเนินการอย่างเหมาะสมหรือเป็นไปตามแนวทางปฏิบัติกระบวนการแลกเปลี่ยน และมาตรฐานตามที่กำหนด

11. การเปิดเผยข้อมูล

เพื่อกำหนดการเปิดเผยข้อมูล เพื่อให้สามารถเปิดเผยข้อมูลได้อย่างถูกต้อง ตรงตามวัตถุประสงค์ของการให้นำข้อมูลไปใช้ประโยชน์ โดยมีรายละเอียด ดังนี้

11.1 ห้ามเปิดเผยข้อมูลที่ขัดต่อกฎหมาย ระเบียบ ข้อบังคับ คำสั่ง นโยบาย แนวปฏิบัติ ไม่ว่าข้อมูลจะอยู่ในรูปแบบใดหรือสถานที่ใดก็ตาม

11.2 ต้องได้รับการอนุญาตจากตัวแทนหน่วยงานหรือเจ้าของข้อมูลก่อนการเปิดเผยข้อมูล

11.3 ควรมีการระบุช่องทางการเปิดเผยข้อมูลที่เข้าถึงและนำไปใช้ได้ง่าย

11.4 ควรมีการเปิดเผยเมทาดาตาควบคู่ไปกับข้อมูลที่เปิดเผย

11.5 สามารถตรวจสอบได้ว่าการเปิดเผยข้อมูลได้ถูกดำเนินการอย่างเหมาะสมหรือเป็นไปตามแนวทางที่ได้กำหนดไว้ เพื่อให้ได้ข้อมูลที่มีคุณภาพ และเป็นการรักษาคุณภาพของข้อมูล

12. การวัดการดำเนินการและความสำเร็จของธรรมาภิบาลข้อมูล

กำหนดให้มีการติดตาม ตรวจสอบ และประเมินผล รวมทั้งการทบทวน การปฏิบัติตามนโยบายธรรมาภิบาลข้อมูลในทุกปี เพื่อให้เห็นระดับการดำเนินการของธรรมาภิบาลข้อมูล ซึ่งจะส่งผลต่อความสำเร็จของการดำเนินการหรือคุณภาพของข้อมูลกลุ่มบริษัท การควบคุมและตรวจสอบการดำเนินงานที่เกี่ยวข้องกับข้อมูล

13. การปฏิบัติและการควบคุมภายใน

13.1 ให้ผู้จัดการเป็นผู้มีอำนาจในการออกระเบียบ หรือคู่มือปฏิบัติงานเพื่อใช้ในการปฏิบัติงานตามนโยบายนี้

13.2 กรณีมีปัญหาเกี่ยวกับการปฏิบัติงานตามนโยบายนี้ ให้ผู้จัดการเป็นผู้วินิจฉัย และให้ถือว่าคำวินิจฉัยของผู้จัดการถือเป็นที่สุด

14. การร้องเรียน การแจ้งเบาะแส

กรณีพบเหตุอันควรสงสัย หรือเชื่อว่ามีการละเมิดการเก็บรวบรวม ใช้ และ/หรือเปิดเผยข้อมูลส่วนบุคคล หรือเจ้าของข้อมูลส่วนบุคคลประสงค์ที่จะร้องเรียน หรือใช้สิทธิของเจ้าของข้อมูลส่วนบุคคลตามนโยบายฉบับนี้ หรือตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 สามารถติดต่อกับเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลของบริษัทตามข้อมูลการติดต่อด้านล่างนี้

คุณธงชัย โตประเสริฐ (IT Manager)
เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล
เลขที่ 968 อาคารอื้อจือเหลียง ชั้นที่ 5 ถนนพระรามที่ 4 แขวงสีลม เขตบางรัก กทม. 10500
Email: thongchai@kratos.co.th เบอร์โทรศัพท์: 0-2095-3200

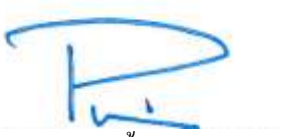
15. การฝ่าฝืน

กลุ่มบริษัทพาราวินเซอร์ จะไม่ยอมประนีประนอมในเรื่องการคุ้มครองข้อมูลส่วนบุคคล หากผู้ควบคุมข้อมูลส่วนบุคคล ผู้ประมวลผลข้อมูล หรือผู้มีหน้าที่รับผิดชอบในการดำเนินงานเรื่องใดเรื่องหนึ่งตามหน้าที่ของตน ที่เกี่ยวข้องกับนโยบายการคุ้มครองข้อมูลส่วนบุคคล ละเลย หรือละเว้นไม่สั่งการ หรือไม่ดำเนินการ หรือสั่งการ หรือดำเนินการอย่างใดอย่างหนึ่งในหน้าที่ของตน จนทำให้เกิดการเก็บรวบรวม ใช้ และ/หรือเปิดเผยข้อมูลส่วนบุคคลโดยผิดวัตถุประสงค์ การละเมิดต่อข้อมูลส่วนบุคคล อันเป็นการฝ่าฝืนนโยบายธรรมาภิบาลข้อมูล และ/หรือตามที่พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 กำหนด พนักงานผู้นั้นต้องรับโทษทางวินัยตาม

ระเบียบของบริษัท และหากการกระทำผิดดังกล่าวของพนักงาน และ/หรือบุคคลใดก่อให้เกิดความเสียหายแก่บริษัท และ/หรือบุคคลใด บริษัทอาจพิจารณาดำเนินคดีตามกฎหมายเพิ่มเติมต่อไป

ทั้งนี้ ให้มีผลบังคับใช้ตั้งแต่วันที่ลงนามเป็นต้นไป

ประกาศ ณ วันที่ 1 มิถุนายน พ.ศ. 2565



(นายประภัสสร์ เอื้อวัฒนสกุล)
กรรมการบริหาร
กลุ่มบริษัทพาราวินเซอร์