



นโยบายการกำหนดชั้นข้อมูลอันเป็นความลับ

ของ

บริษัท โซลาร์ตรอน จำกัด (มหาชน)

และบริษัทในเครือ

สารบัญ

	หน้า
1. หลักการและเหตุผล	1
2. วัตถุประสงค์	1
3. ขอบเขตการบังคับใช้	1
4. คำนิยามที่เกี่ยวข้อง	1
5. หลักการกำหนดชั้นความลับของข้อมูล	3
6. ประเภทของชั้นความลับ	4
7. การปกป้องข้อมูลองค์กรมิให้รั่วไหลโดยแบ่งชั้นข้อมูล (Data Classification)	4
8. แนวปฏิบัติที่ดี	6
9. ช่องทางการติดต่อ	7
10. การติดตามผล การทบทวนและการปรับปรุง	7
11. บทลงโทษ	7

นโยบายการกำหนดชั้นข้อมูลอันเป็นความลับ

1. หลักการและเหตุผล

บริษัท โซลาร์ตรอน จำกัด (มหาชน) และบริษัทในเครือ ตระหนักถึงความสำคัญของการบริหารจัดการข้อมูลและสารสนเทศขององค์กร ซึ่งเป็นทรัพยากรที่มีคุณค่าและมีความจำเป็นต่อการดำเนินธุรกิจ การตัดสินใจเชิงบริหาร การให้บริการแก่ลูกค้า ตลอดจนการปฏิบัติตามกฎหมายและข้อกำหนดที่เกี่ยวข้อง ข้อมูลบางประเภทมีความอ่อนไหวและอาจก่อให้เกิดผลกระทบต่อบริษัท คู่ค้า ลูกค้า หรือบุคคลที่เกี่ยวข้อง หากมีการเปิดเผย เปลี่ยนแปลง ทำลาย หรือเข้าถึงโดยไม่ได้รับอนุญาต ดังนั้น การกำหนดชั้นความลับของข้อมูลจึงเป็นกลไกสำคัญในการคุ้มครองข้อมูลให้มีความมั่นคงปลอดภัย เหมาะสมตามระดับความสำคัญและความเสี่ยง รวมทั้งสนับสนุนให้การดำเนินงานของบริษัทเป็นไปอย่างมีประสิทธิภาพ โปร่งใส และต่อเนื่อง

บริษัทจึงจัดทำนโยบายการกำหนดชั้นข้อมูลอันเป็นความลับฉบับนี้ขึ้น เพื่อกำหนดหลักเกณฑ์ วิธีการ และมาตรการควบคุมในการจำแนกข้อมูลตามระดับชั้นความลับ การจัดการ การเข้าถึง การใช้ การจัดเก็บ การส่งต่อ ตลอดจนการทำลายข้อมูลอย่างเหมาะสม โดยอ้างอิงจากหลักปฏิบัติด้านความมั่นคงปลอดภัยสารสนเทศที่เป็นที่ยอมรับ แนวทางกำกับดูแลกิจการที่ดี ข้อกำหนดของหน่วยงานกำกับดูแลที่เกี่ยวข้อง และกฎหมายต่าง ๆ อาทิ กฎหมายคุ้มครองข้อมูลส่วนบุคคล กฎหมายว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ และข้อกำหนดตามสัญญาทางธุรกิจ เพื่อนำมาปรับใช้ให้สอดคล้องกับบริบทการดำเนินธุรกิจของบริษัท และเพื่อให้พนักงานทุกระดับ รวมถึงผู้เกี่ยวข้องภายนอกที่ได้รับข้อมูลของบริษัท สามารถปฏิบัติได้อย่างถูกต้องเป็นมาตรฐานเดียวกัน ลดความเสี่ยงจากการรั่วไหลของข้อมูล เสริมสร้างความเชื่อมั่นต่อผู้มีส่วนได้เสีย และคุ้มครองผลประโยชน์ของบริษัทอย่างยั่งยืน

2. วัตถุประสงค์

นโยบายฉบับนี้จัดทำขึ้นเพื่อใช้เป็นเกณฑ์พิจารณากำหนดชั้นความลับสำหรับทุกชุดข้อมูล เพื่อลดการใช้ดุลพินิจของผู้มีอำนาจในการตัดสินใจในการตัดสินใจกำหนดชั้นความลับของข้อมูล การรักษาความปลอดภัยของข้อมูล รวมถึงการเข้าถึงข้อมูลตามระดับชั้นความลับ โดยให้มีระบบบริหารจัดการคุ้มครองข้อมูลที่เหมาะสม มีการกำหนดมาตรการและหน้าที่ความรับผิดชอบที่จำเป็นในการรักษาความปลอดภัยของข้อมูล เพื่อบริหารจัดการให้สอดคล้องตามกฎหมาย

3. ขอบเขตการบังคับใช้

นโยบายฉบับนี้มีผลบังคับใช้กับบริษัท โซลาร์ตรอน จำกัด (มหาชน) และบริษัทในเครือ โดยนโยบายหลักเกณฑ์ระเบียบปฏิบัติและคำสั่งที่ใช้อยู่ก่อนนโยบายฉบับนี้ ให้ยังมีผลใช้บังคับต่อไปเท่าที่ไม่ขัดหรือแย้งกับนโยบายฉบับนี้

4. คำนิยามที่เกี่ยวข้อง

“บริษัท”

หมายถึง บริษัท โซลาร์ตรอน จำกัด (มหาชน)

“บริษัทในเครือ”

หมายถึง บริษัทในเครือที่บริษัทมีอำนาจควบคุม ได้แก่ บริษัท โซลาร์ตรอน เอ็นเนอร์ยี 1 จำกัด และบริษัท โซลาร์ตรอน เอ็นเนอร์ยี 3 จำกัด

“ผู้บริหาร”	หมายถึง ผู้บริหารบริษัท โซลาร์ตรอน จำกัด (มหาชน) และบริษัทในเครือ ระดับผู้จัดการฝ่ายขึ้นไป
“บุคลากรของโซลาร์ตรอน”	หมายถึง กรรมการ ผู้บริหาร และพนักงานทุกระดับของ กลุ่มบริษัทโซลาร์ตรอน รวมถึงลูกจ้างโครงการ ลูกจ้างชั่วคราว และลูกจ้างรายวันตามสัญญาจ้าง
“นโยบาย”	หมายถึง นโยบายการกำหนดชั้นข้อมูลอันเป็นความลับ
“การกำหนดชั้นความลับของข้อมูล”	หมายถึง การจำแนกชั้นของข้อมูลในบริบทของการรักษาความปลอดภัยข้อมูลตามระดับของความอ่อนไหวและผลกระทบต่อบุคคล และองค์กร หากมีการเปิดเผยเปลี่ยนแปลงหรือทำลายข้อมูลโดยไม่ได้รับอนุญาต โดยการจัดชั้นความลับของข้อมูลช่วยกำหนดการควบคุมความปลอดภัยพื้นฐานที่เหมาะสมสำหรับการปกป้องข้อมูลนั้น ๆ
“ข้อมูลอ่อนไหว”	หมายถึง ข้อมูลอ่อนไหวเป็นข้อมูลที่มีชั้นความลับและเป็นข้อมูลที่ต้องได้รับการป้องกันจากการเข้าถึงโดยไม่ได้รับอนุญาต เพื่อคุ้มครองความเป็นส่วนตัว หรือความปลอดภัยของบุคคลหรือองค์กร และให้หมายรวมถึงข้อมูลส่วนบุคคลชนิดพิเศษ ตามกฎหมายคุ้มครองข้อมูลส่วนบุคคลด้วย
“ข้อมูลส่วนบุคคล”	หมายถึง ข้อมูลที่เกี่ยวกับบุคคลธรรมดา ซึ่งทำให้สามารถระบุตัวตนของบุคคลนั้นได้ไม่ว่าทางตรงหรือทางอ้อม เช่น ชื่อ-นามสกุล อีเมล ที่อยู่ เบอร์โทรศัพท์ ที่อยู่ จดหมายอิเล็กทรอนิกส์ที่ระบุตัวบุคคลธรรมดา IP Address รูปภาพบุคคล ซึ่งเกี่ยวข้องกับการดำเนินการต่าง ๆ ของกลุ่มธุรกิจบริษัทและบริษัทในเครือ เช่น ข้อมูลที่เกี่ยวข้องกับการจัดซื้อ จัดจ้าง และบริการอื่น ๆ เป็นต้น
“ข้อมูลอันเป็นความลับ”	หมายถึง ข้อมูลข่าวสารลับที่มีค่าส่งไม่ให้เกิดเปิดเผยและอยู่ในความครอบครองหรือควบคุมดูแลของบริษัทและบริษัทในเครือซึ่งมีการกำหนดให้มีชั้นความลับ ตามแนวปฏิบัติฉบับนี้โดยคำนึงถึงการปฏิบัติหน้าที่ของหน่วยงานของบริษัทและประโยชน์ของบริษัทประกอบกัน
“ข้อมูลลับ”	หมายถึง ข้อมูลที่ยังมิได้มีการเปิดเผยต่อสาธารณชนหรือผ่านระบบของตลาดหลักทรัพย์เป็นการทั่วไป ซึ่งเป็นสาระสำคัญต่อการเปลี่ยนแปลงของราคาหรือมูลค่าของหลักทรัพย์ และการตัดสินใจซื้อขายหลักทรัพย์ ตัวอย่างของข้อมูลภายใน ได้แก่ 1) ฐานะทางการเงินและผลประกอบการทางการเงิน 2) การจ่ายหรือไม่จ่ายเงินปันผล 3) การเปลี่ยนแปลงมูลค่าที่ตราไว้ของหลักทรัพย์ 4) แผนธุรกิจและแผนการระดมทุน การเพิ่ม/ลดทุนโดยใช้เครื่องมือทางการเงิน 5) การเปลี่ยนแปลงที่สำคัญในแผนการลงทุน หรือโครงการลงทุน 6) การร่วมทุน การควบรวมกิจการ หรือการขายกิจการ 7) การซื้อขายหลักทรัพย์ที่สำคัญ และการไถ่ถอนหลักทรัพย์ 8) การได้มาหรือสูญเสียสัญญาทางการค้าที่สำคัญของบริษัทและบริษัทในเครือ 9) ข้อพิพาททางกฎหมายที่สำคัญ 10) การเปลี่ยนแปลงวัตถุประสงค์ของบริษัทและบริษัทในเครือ 11) การเปลี่ยนแปลงนโยบายการบัญชีที่สำคัญ 12) การเปลี่ยนแปลงอำนาจควบคุม หรือการเปลี่ยนแปลงที่สำคัญในคณะกรรมการบริษัท หรือผู้บริหารระดับสูง

“ข้อมูล”

หมายถึง ข้อมูล ข้อความ คำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใดบรรดาที่อยู่ในระบบคอมพิวเตอร์ในสภาพที่ระบบคอมพิวเตอร์อาจประมวลผลได้ และให้หมายความรวมถึงข้อมูลอิเล็กทรอนิกส์ตามกฎหมายว่า ด้วยธุรกรรมทางอิเล็กทรอนิกส์และข้อมูลส่วนบุคคลตามกฎหมายคุ้มครองข้อมูลส่วนบุคคลด้วย

“ข้อมูลสารสนเทศ”

หมายถึง ข้อมูลที่ผ่านการประมวลผลแล้ว การจัดระเบียบให้ข้อมูลซึ่งอยู่ในรูปตัวเลข ข้อความหรือกราฟิก ให้อยู่ในลักษณะที่ผู้ใช้สามารถเข้าใจได้ง่าย และสามารถนำไปใช้ประโยชน์ในการบริหาร การวางแผน การตัดสินใจ และอื่น ๆ ได้ รวมถึงข้อมูลส่วนบุคคล

“ความลับทางการค้า”

หมายถึง ข้อมูลการค้าซึ่งยังไม่รู้จักกันโดยทั่วไป หรือยังเข้าถึงไม่ได้ในหมู่บุคคลซึ่งโดยปกติแล้วต้องเกี่ยวข้องกับข้อมูลดังกล่าว โดยเป็นข้อมูลที่มีประโยชน์ในเชิงพาณิชย์ เนื่องจากการเป็นความลับ และเป็นข้อมูลที่ผู้ควบคุมความลับทางการค้าได้ใช้ มาตรการที่เหมาะสมเพื่อรักษาไว้เป็นความลับ

“ข้อมูลการค้า”

หมายถึง สิ่งที่สื่อความหมายให้รู้ข้อความ เรื่องราวข้อเท็จจริง หรือสิ่งใดไม่ว่าการสื่อความหมายนั้นและผ่านวิธีการใด ๆ และไม่ว่าจะจัดไว้ในรูปใด ๆ และให้หมายความรวมถึง สูตร รูปแบบ งานที่ได้รวบรวมหรือประกอบขึ้น โปรแกรม วิธีการ เทคนิค หรือกรรมวิธี ด้วย (พรบ.ความลับทางการค้า พ.ศ.2545)

“การเปิดเผยข้อมูลความลับ”

หมายถึง การเผยแพร่ การขาย การให้เข้าซื้อ การแจกจ่าย การทำซ้ำ การดัดแปลง และการให้เข้าต้นฉบับหรือสำเนา งาน ที่เกี่ยวข้องกับ “ข้อมูลอันเป็นความลับ” ไม่ว่าทั้งหมดหรือบางส่วน ไม่ว่าจะอยู่ในลักษณะที่อาจก่อให้เกิดความเสียหายแก่ผู้ให้ข้อมูลหรือไม่ก็ตาม

“การปรับขึ้นความลับ”

หมายถึง การลดหรือเพิ่มชั้นความลับของข้อมูลข่าวสารลับ และให้หมายความรวมถึงการยกเลิกชั้นความลับของข้อมูลข่าวสารลับนั้นด้วย

5. หลักการกำหนดชั้นความลับของข้อมูล

- 5.1 บริษัทใช้ความระมัดระวังในการจำแนกชั้นความลับ ความสอดคล้องกับความอ่อนไหว และความสำคัญของข้อมูล ในการจำกัดการเข้าถึงข้อมูลจะพิจารณาในกรณีที่เป็นการเปิดเผยข้อมูลที่อาจส่งผลกระทบต่อกฎหมาย ชื่อเสียง และผลประโยชน์ของบริษัท
- 5.2 การกำหนดชั้นความลับของข้อมูล จะพิจารณาตามเนื้อหาและความเสี่ยงที่ส่งผลกระทบต่อกฎหมาย ชื่อเสียง และผลประโยชน์ของบริษัท หรืออื่น ๆ ที่เกี่ยวข้อง โดยไม่คำนึงถึงรูปแบบ หรือแหล่งที่มาของข้อมูล ที่มีจัดเก็บไว้ในระบบฐานข้อมูลของบริษัท ไม่ว่าเป็นการจัดเก็บในรูปแบบ Hard Copy หรือ Electronic file ก็ตาม
- 5.3 บริษัท จัดให้มีแนวทางการบริหารความเสี่ยงของข้อมูลที่ควรได้รับความคุ้มครองตามระดับความอ่อนไหวและความสำคัญของข้อมูล เพื่อกำหนดขอบเขตของมาตรการในการลดความเสี่ยงให้อยู่ในระดับที่ยอมรับได้ อาทิ ความรุนแรง และความเป็นไปได้ที่ข้อมูลจะถูกถูกลักหรือถูกทำลาย หรือระดับความเสียหายที่อาจเกิดขึ้น เป็นต้น
- 5.4 การกำหนดระดับชั้นของข้อมูลต้องมีความเหมาะสม เพื่อให้ผู้เกี่ยวข้องได้ใช้ประโยชน์จากข้อมูลให้ได้มากที่สุด โดยมีตั้งแต่ระดับต่ำที่สุด ไปจนถึงระดับข้อมูลที่สำคัญสูง ซึ่งระดับที่สำคัญสูงจะต้องได้รับการปกป้องเพื่อรักษาความปลอดภัยของข้อมูล
- 5.5 ในการบริหารจัดการระบบควบคุมภายในให้เป็นไปอย่างเหมาะสม บริษัท ได้กำหนดบทบาทหน้าที่ของ ผู้มีส่วนเกี่ยวข้องกับข้อมูลที่ชัดเจน ตลอดจนสร้างความตระหนักรู้ในการบริหารจัดการและมุ่งมั่นในการรักษาความปลอดภัยของข้อมูล

6. ประเภทของชั้นความลับ

1. ชั้นเปิดเผย (Open/Public) หมายถึง ข้อมูลที่สามารถเปิดเผย หรือเผยแพร่ทั่วไปได้ทั้งภายใน ภายนอก โดยไม่จำกัดการเข้าถึง
2. ชั้นถูกจำกัด & ชั้นเผยแพร่ภายในองค์กร (Private) หมายถึง ข้อมูลที่จำกัดการเข้าถึง หรือต้องได้รับการอนุญาตจากเจ้าของข้อมูลก่อน มีการเข้ารหัสและแยกอีเมลรหัสกับอีเมลข้อมูล หรือข้อมูลที่ไม่ได้เผยแพร่โดยอิสระ การเปิดเผยจะกระทำได้ต่อเมื่อได้รับการอนุญาตจากผู้มีอำนาจเท่านั้น และการกระทำนั้นต้องไม่ส่งผลกระทบต่อบริษัทและบริษัทในเครือ
3. ชั้นความลับที่มีระดับสูง & ข้อมูลอ่อนไหว และมีผลกระทบต่อสิทธิเสรีภาพ หมายถึง ข้อมูลลับที่มีระดับสูงสุด ซึ่งหากเปิดเผยอาจก่อให้เกิดความเสียหายต่อบริษัทได้ ต้องมีการจำกัดการเข้าถึงอย่างเข้มงวด ต้องได้รับอนุญาตจากเจ้าของข้อมูล มีการเข้ารหัสและแยกอีเมลรหัสกับอีเมลข้อมูล และมีแผนปฏิบัติการฉุกเฉิน รองรับความเสี่ยง เพื่อความปลอดภัยของข้อมูล ซึ่งรวมถึงข้อมูลอ่อนไหว ข้อมูลส่วนบุคคลชนิดพิเศษตามกฎหมายคุ้มครองข้อมูลส่วนบุคคล

7. การปกป้องข้อมูลองค์กรมิให้รั่วไหลโดยแบ่งชั้นข้อมูล (Data Classification)

รายการ	ชั้นความลับที่มีระดับสูง & ข้อมูลอ่อนไหวและมีผลกระทบต่อสิทธิเสรีภาพ	ชั้นถูกจำกัด & ชั้นเผยแพร่ภายในองค์กร	ชั้นเปิดเผย
คำอธิบาย	ข้อมูลที่ได้รับควบคุมคุ้มครองตามกฎหมาย และข้อมูลที่ต้องกำหนดสิทธิในการเข้าถึง หรือข้อมูลที่ถูกจำกัด	ข้อมูลที่ผู้จัดการหน่วยงานไม่มีอำนาจตัดสินใจให้เผยแพร่หรือเปิดเผยต่อสาธารณะ หรือข้อมูลที่ได้รับการคุ้มครองตามข้อผูกพันตามสัญญา หรือข้อมูลที่เผยแพร่ภายในองค์กรเท่านั้น	ข้อมูลที่ไม่มีความเป็นส่วนตัวหรือเป็นความลับ
ข้อบังคับทางกฎหมาย	มีกฎหมายกำหนดให้ต้องมีการคุ้มครองข้อมูล	การคุ้มครองข้อมูล ขึ้นอยู่กับดุลยพินิจของผู้จัดการหรือผู้ดูแลข้อมูล	
ความเสี่ยงที่ส่งผลกระทบต่อชื่อเสียง / ผลประโยชน์ของบริษัท	มีความเสี่ยงสูง (High)	ปานกลาง (Medium)	ต่ำ (Low)
การควบคุมการเข้าถึงระบบสารสนเทศ	ข้อมูลซึ่งอยู่ภายใต้ข้อจำกัดทางกฎหมาย จริยธรรมหรือข้อกำหนดอื่น อนุญาตให้เข้าถึงได้เฉพาะผู้ได้รับอนุมัติเป็นการเฉพาะ และได้ลงนามในข้อตกลงรักษาความลับแล้วเท่านั้น	การเข้าถึงได้เฉพาะพนักงานที่มีหน้าที่เกี่ยวข้องเท่านั้น	ไม่มีจำกัดการเข้าถึงข้อมูลสามารถเข้าถึงได้โดยอิสระ
กลไกการรับ-ส่งข้อมูล	ห้ามส่งข้อมูลลับในระดับนี้ผ่านเครือข่ายที่ไม่ใช่เครือข่ายหลักของบริษัท การรับ-ส่งทั้งภายในและ	ไม่แนะนำให้ส่งข้อมูลที่มีข้อจำกัดผ่านเครือข่ายไร้สายหรือเครือข่ายแบบใช้สาย (LAN) ที่ไม่ใช่ของบริษัท	ข้อมูลที่เปิดเผยหรือเป็นสาธารณะไม่จำเป็นต้องมีการป้องกันเป็นพิเศษ อย่างไรก็ตาม

รายการ	ชั้นความลับที่มีระดับสูง & ข้อมูลอ่อนไหวและมีผลกระทบต่อสิทธิเสรีภาพ	ชั้นถูกจำกัด & ชั้นเผยแพร่ภายในองค์กร	ชั้นเปิดเผย
	ภายนอกต้องดำเนินการผ่านอีเมลของบริษัทเท่านั้นโดยต้องได้รับอนุญาตจากเจ้าของข้อมูล พร้อมเข้ารหัสข้อมูล และแยกการส่งรหัสผ่านออกจากอีเมลข้อมูล"	หากมีความจำเป็นต้องใช้ ให้ดำเนินการผ่าน VPNของบริษัทเท่านั้น การรับ-ส่งข้อมูลทั้งภายในและภายนอกต้องใช้อีเมลของบริษัท และได้รับอนุญาตจากเจ้าของข้อมูลก่อนทุกครั้ง	ควรใช้ข้อมูลทั้งหมดของบริษัทด้วยความระมัดระวังและเหมาะสม
การจัดเก็บข้อมูล	- ห้ามจัดเก็บข้อมูลที่เป็นความลับในระดับชั้นนี้ไว้ในเครื่อง/อุปกรณ์คอมพิวเตอร์ - จัดเก็บในฐานข้อมูลส่วนกลาง - ต้องมีการเข้ารหัสที่ได้รับการอนุมัติบนอุปกรณ์คอมพิวเตอร์พกพา	- มีการกำหนดสิทธิเข้าถึงข้อมูล ซึ่งจะต้องได้รับการพิจารณาอนุญาตจากผู้มีอำนาจ หรือเจ้าของข้อมูล หรือผู้ดูแลระบบที่ได้รับมอบหมายเป็นลายลักษณ์อักษร - มีระบบรักษาความปลอดภัยในการจัดเก็บข้อมูล - ข้อมูลที่ยังไม่เปิดเผยต่อสาธารณะต้องปฏิบัติตามขั้นตอนการรักษาความปลอดภัยโดยเคร่งครัด	ข้อมูลที่เปิดเผยหรือเป็นสาธารณะไม่จำเป็นต้องมีการป้องกันเป็นพิเศษ อย่างไรก็ตามควรใช้ข้อมูลทั้งหมดของบริษัทด้วยความระมัดระวังและเหมาะสม
การสำรอง และการกู้คืนเอกสาร	จำเป็นต้องมีขั้นตอนการปฏิบัติงานในการสำรองและการกู้คืนเอกสาร	ไม่จำเป็นต้องมีขั้นตอนการปฏิบัติงานในการสำรองและการกู้คืนเอกสาร แต่ควรระบุวิธีการจัดเก็บเอกสารอย่างเป็นระบบ	
การเก็บรักษาข้อมูลที่เป็นเอกสาร	จำเป็นต้องมีแนวปฏิบัติในการเก็บรักษาข้อมูลที่เป็นเอกสาร		ไม่จำเป็นต้องมีแนวปฏิบัติในการเก็บรักษาข้อมูลที่เป็นเอกสาร แต่ควรระบุวิธีการจัดเก็บเอกสารอย่างเป็นระบบ
ระบบควบคุมภายใน	ผู้จัดการ/ผู้ดูแลข้อมูลที่มีหน้าที่รับผิดชอบข้อมูลที่เป็นความลับต้องตรวจสอบและทบทวนระบบและขั้นตอนสำหรับการใช้ข้อมูลในทางที่ผิดและ/หรือการเข้าถึงโดยไม่ได้รับอนุญาต พร้อมรายงานความผิดปกติให้กับเจ้าหน้าที่ระบบเทคโนโลยีสารสนเทศเพื่อวิเคราะห์ หาแนวทางแก้ไข หรือกำหนดแนวทางปฏิบัติด้านความปลอดภัยของหน่วยงาน	ผู้จัดการ/ผู้ดูแลข้อมูล ซึ่งรับผิดชอบข้อมูลที่ถูกต้องจะต้องตรวจสอบและทบทวนระบบและขั้นตอนของตนเป็นระยะ ๆ สำหรับการใช้ในทางที่ผิดและ/หรือการเข้าถึงโดยไม่ได้รับอนุญาต	ไม่จำเป็นต้องมีการตรวจสอบโดยผู้ควบคุมข้อมูล

8. แนวปฏิบัติที่ดี

- 8.1 บุคลากร พนักงาน ที่สามารถเข้าถึงข้อมูลอันเป็นความลับ ในชั้นความลับใดก็ตาม จะต้องเป็นบุคคลที่ผู้บังคับบัญชามอบหมาย ความไว้วางใจ และให้เข้าถึงข้อมูลอันเป็นความลับ ได้เฉพาะเรื่องที่ได้รับมอบหมายเท่านั้น และมีหน้าที่รักษาความลับและความปลอดภัยของข้อมูล เพื่อปกป้องข้อมูลอันเป็นความลับ และเพื่อไม่ให้ข้อมูลอันเป็นความลับถูกเปิดเผย
- 8.2 ข้อมูลที่เป็นความลับและข้อมูลที่ถูกจำกัดต้องได้รับการเก็บรักษาอย่างปลอดภัย ถูกต้อง และเชื่อถือได้ และพร้อมสำหรับการใช้งาน โดยผู้ที่ได้รับอนุญาตมีมาตรการรักษาความปลอดภัยที่แตกต่างกันไป ตามความเหมาะสมกับระดับที่ข้อมูลจะสูญหายหรือเสียหาย หรือทำให้ธุรกิจเสื่อมเสีย เสียหาย หรือละเมิดกฎหมายนโยบาย หรือสัญญา มาตรการรักษาความปลอดภัยของข้อมูล กำหนดโดยเจ้าหน้าที่ระบบเทคโนโลยีสารสนเทศ และผู้จัดการหน่วยงานที่ดูแลข้อมูล
- 8.3 การกำหนดมาตรการรักษาความปลอดภัยของข้อมูล ต้องมีการประเมินความเสี่ยงด้านมูลค่าของข้อมูล ความละเอียดอ่อน ชื่อเสียง หรือผลประโยชน์ของบริษัท เพื่อใช้การรักษาความปลอดภัยในระดับที่เหมาะสม
- 8.4 กำหนดให้ผู้จัดการหน่วยงาน มีหน้าที่รักษาดูแลข้อมูลอันเป็นความลับ โดยจัดทำตารางควบคุมรายการเอกสารข้อมูลอันเป็นความลับในหน่วยงานของตน ตามแบบฟอร์มที่บริษัทกำหนดไว้ โดยจะต้องรักษาข้อมูลอันเป็นความลับให้ปลอดภัย การจำกัดบุคคลเข้าถึงข้อมูลอันเป็นความลับ หรือหากมีการเปิดเผยข้อมูลอันเป็นความลับแก่ผู้ใด ต้องกระทำโดยระมัดระวัง พร้อมจัดทำแผนปฏิบัติการฉุกเฉินกรณีข้อมูลอันเป็นความลับที่มีความเสี่ยงสูง เกิดการรั่วไหล หรือถูกโจรกรรมข้อมูล หรือข้อมูลสูญหายให้สอดคล้องตามนโยบายของบริษัท
- 8.5 จัดให้มีการตรวจสอบข้อมูลที่ได้รับการจัดชั้นความลับ เพื่อให้แน่ใจว่าข้อมูลอันเป็นความลับได้ถูกจัดเก็บอย่างเหมาะสม ปลอดภัย และมีแผนรองรับความเสี่ยงของข้อมูลความลับที่มีความเสี่ยงสูงนั้น ๆ หากพบว่ามีการจัดการข้อมูลไม่ถูกต้องหรือไม่เหมาะสม ให้แจ้งผู้เกี่ยวข้องรับผิดชอบดำเนินการแก้ไขทันที
- 8.6 กำหนดให้เจ้าหน้าที่ระบบเทคโนโลยีสารสนเทศ มีหน้าที่กำหนดสิทธิ์การเข้าถึงและการนำข้อมูลไปใช้อย่างเหมาะสม โดยได้รับการอนุมัติจากผู้จัดการหน่วยงานก่อนที่จะให้สิทธิ์ในการเข้าถึง และทบทวนสิทธิ์การเข้าถึงอย่างน้อยปีละ 1 ครั้ง รวมถึงรับผิดชอบทางเทคนิคขั้นสูงสำหรับการปกป้องคุ้มครองข้อมูล เพื่อให้การดำเนินงานด้านเทคโนโลยีมีประสิทธิภาพ
- 8.7 หากพบว่าข้อมูลสูญหาย ถูกลบหรือถูกละเมิดข้อมูล ให้ผู้ทราบข้อเท็จจริงรายงานข้อเท็จจริงที่เกี่ยวข้องให้ผู้จัดการทราบ เพื่อพิจารณารายงานการละเมิด
 - กรณีข้อมูลที่จัดอยู่ในรูปแบบ Electronic file และอยู่ในระบบคลาวด์ของบริษัท ให้แจ้งไปยังเจ้าหน้าที่ระบบเทคโนโลยีสารสนเทศดำเนินการตรวจสอบการกระทำที่เกี่ยวกับข้อมูลที่ถูกละเมิดนั้น ประเมินผลกระทบที่เกิดขึ้นและรายงานไปยังผู้บริหารสูงสุดสายงานเทคโนโลยีสารสนเทศเพื่อรายงานต่อคณะกรรมการบริหาร ทั้งนี้ให้ปฏิบัติตามนโยบายและแนวปฏิบัติด้านเทคโนโลยีสารสนเทศที่เกี่ยวข้อง
 - กรณีข้อมูลที่อยู่ในประเภท Hard Copy หากพบว่าข้อมูลสูญหาย ถูกลบหรือถูกทำลาย โดยไม่ชอบให้ผู้พบเห็นแจ้งเหตุไปยังหน่วยงานตรวจสอบภายใน เพื่อดำเนินการสอบสวนหาข้อเท็จจริง และรายงานผลต่อคณะกรรมการบริหาร และคณะกรรมการตรวจสอบทราบ
- 8.8 จัดให้มีการสื่อสารและฝึกอบรมอย่างต่อเนื่องแก่พนักงาน เพื่อให้เกิดความรู้ ความเข้าใจอย่างแท้จริง เกี่ยวกับมาตรการและความรับผิดชอบที่จำเป็นสำหรับการรักษาความปลอดภัยของข้อมูล ความคาดหวัง และบทลงโทษหากไม่ปฏิบัติตามนโยบายฉบับนี้

9. ช่องทางการติดต่อ

บริษัท กำหนดให้หน่วยงานกำกับและควบคุม มีหน้าที่ให้คำปรึกษาและข้อเสนอแนะเกี่ยวกับนโยบายฉบับนี้ เพื่อให้การปฏิบัติงานสอดคล้องตามหลักการกำหนดชั้นความลับของข้อมูล และตามหลักการกำกับดูแลกิจการที่ดี

10. การติดตามผล การทบทวนและการปรับปรุง

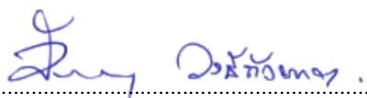
บริษัท กำหนดให้หน่วยงานตรวจสอบภายใน มีหน้าที่สอบทานความเพียงพอ เหมาะสมและประสิทธิภาพของระบบควบคุมภายใน และการปฏิบัติตามนโยบายฉบับนี้ หากพบว่ามีบุคคลที่ไม่มีอำนาจหน้าที่เกี่ยวข้องกับข้อมูลอันเป็นความลับได้รู้หรืออาจรู้ถึงข้อมูลอันเป็นความลับ หรือเมื่อสงสัยว่ามีการละเมิดการรักษาความลับของข้อมูลข่าวสารของบริษัท ให้ดำเนินการสอบสวนโดยไม่ชักช้า และรายงานผลต่อคณะกรรมการตรวจสอบทราบ

11. บทลงโทษ

หากพบว่าพนักงาน หรือผู้ที่เกี่ยวข้อง มีการละเมิด หรือไม่ปฏิบัติตามมาตรการตามนโยบายฉบับนี้และนโยบายที่เกี่ยวข้องกับนโยบายนี้ พนักงานหรือผู้เกี่ยวข้องนั้นอาจถูกระงับหรือการยุติการเข้าถึง และอาจมีการลงโทษทางวินัย ตามระเบียบข้อบังคับ หรือตามที่กำหนดไว้ในนโยบายที่เกี่ยวข้องอื่น ๆ หรือมีโทษทางแพ่งหรือทางอาญาตามแต่กรณี

จึงประกาศมาเพื่อทราบโดยทั่วกัน

ประกาศ ณ วันที่ 6 พฤษภาคม พ.ศ. 2568

ลงชื่อ.....

(นางปัทมา วงษ์ฉ่วยทอง)

ประธานเจ้าหน้าที่บริหาร