



นโยบายและแนวปฏิบัติเกี่ยวกับชั้นความลับของข้อมูล

Data Classification Policy and Guidelines

---

บริษัท ปิ่นทอง อินดัสเตรียล พาร์ค จำกัด (มหาชน)

วันที่ 14 พฤศจิกายน 2568

อนุมัติเมื่อ 14 พ.ย. 2568 (BOD 4/2568)

## นโยบายและแนวปฏิบัติเกี่ยวกับชั้นความลับของข้อมูล

บริษัท ปิ่นทอง อินดัสเตรียล ปาร์ค จำกัด (มหาชน) และบริษัทย่อย (“บริษัทฯ”) ตระหนักดีว่าข้อมูลสารสนเทศทุกรูปแบบเป็นทรัพยากรที่มีความสำคัญอย่างยิ่งต่อการดำเนินงาน การบริหาร และการจัดการในทุกระดับขององค์กร การบริหารจัดการข้อมูลอย่างเหมาะสมจึงเป็นสิ่งจำเป็น เพื่อให้การดำเนินธุรกิจเป็นไปอย่างมีประสิทธิภาพ โปร่งใส และปลอดภัย

ในการพิจารณาว่าข้อมูลใดควรจัดเป็นข้อมูลที่เป็นความลับหรือไม่ บริษัทฯ จะพิจารณาจากปัจจัยสำคัญ ได้แก่ ความสำคัญและคุณค่าของข้อมูล กฎหมาย แหล่งที่มา วิธีการนำไปใช้ประโยชน์ จำนวนผู้ที่สามารถเข้าถึง รวมถึงผลกระทบที่อาจเกิดขึ้นหากข้อมูลถูกเปิดเผยหรือถูกเปลี่ยนแปลงโดยไม่ได้รับอนุญาต ทั้งนี้ ข้อมูลดังกล่าวต้องได้รับการควบคุมและอนุมัติจากหน่วยงานเจ้าของข้อมูลหรือผู้มีอำนาจที่บริษัทฯ กำหนด

เพื่อคุ้มครองข้อมูลของบริษัทฯ จากความเสียหาย การเข้าถึงโดยไม่ชอบ การเปิดเผย การเปลี่ยนแปลง หรือการนำไปใช้โดยไม่ได้รับอนุญาต บริษัทฯ จึงได้จัดทำนโยบายและแนวปฏิบัติเกี่ยวกับชั้นความลับของข้อมูล (Data Classification Policy and Guidelines) เพื่อกำหนดหลักเกณฑ์และแนวปฏิบัติที่ชัดเจนในการจำแนกประเภทของข้อมูลตามระดับชั้นความลับ และการกำหนดมาตรการควบคุมการเข้าถึงข้อมูลให้เหมาะสมกับระดับความสำคัญของข้อมูลนั้นๆ

### คำนิยาม

“บริษัทฯ” หมายถึง บริษัท ปิ่นทอง อินดัสเตรียล ปาร์ค จำกัด (มหาชน) และ บริษัทย่อย

“ข้อมูล” หมายถึง ข้อเท็จจริง รายละเอียด หรือสัญลักษณ์ใดๆ ไม่ว่าจะอยู่ในรูปแบบ ตัวอักษร ตัวเลข รูปภาพ เสียง หรือสื่ออื่นใด ที่สามารถบันทึก จัดเก็บ ประมวลผลวิเคราะห์ หรือใช้ประโยชน์ได้โดยรวมถึงข้อมูลที่เป็นข้อมูลทั่วไป หรือเปิดเผยต่อสาธารณะได้ หรือ เป็นข้อมูลที่ต้องมีการควบคุมการเข้าถึง เช่น ข้อมูลส่วนบุคคล ข้อมูลทางธุรกิจ หรือข้อมูลความลับขององค์กร

“ข้อมูลส่วนบุคคล” หมายถึง ข้อมูลใดๆ ที่เกี่ยวข้องกับบุคคลธรรมดา ซึ่งสามารถระบุถึงตัวตนของเจ้าของข้อมูลไม่ว่าจะโดยตรงและโดยอ้อม ตามนิยามที่บัญญัติไว้ในพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

“ข้อมูลทั่วไป (Public)” หมายถึง ข้อมูลทั่วไปที่บริษัทฯ ต้องเผยแพร่ต่อสาธารณะ ลูกค้า หรือ บุคคลภายนอกอยู่แล้ว หรือเป็นข้อมูลที่บุคคลภายนอกทั่วไปสามารถทราบได้โดยไม่ต้องมีการปิดกั้น หรือเป็นข้อมูลที่กฎหมายระบุว่าต้องเปิดเผย

**“ข้อมูลภายใน (Internal)”** หมายถึง ข้อมูลที่จัดทำขึ้นเพื่อใช้ภายในองค์กรเท่านั้น โดยพนักงานได้รับอนุญาตให้ใช้เพื่อปฏิบัติงานตามหน้าที่ที่ได้รับมอบหมาย กรณีที่มีการเปิดเผยข้อมูลต่อบุคคลภายนอกบริษัท จะทำได้ต่อเมื่อได้รับอนุญาตจากหน่วยงานเจ้าของข้อมูลหรือผู้มีอำนาจที่บริษัทฯ กำหนด

**“ข้อมูลเฉพาะกลุ่ม (Restricted)”** หมายถึง ข้อมูลที่บริษัทฯ ไม่สามารถเปิดเผยให้พนักงานทุกคนทราบ เป็นข้อมูลสำคัญสูงสุดโดยกำหนดให้เฉพาะผู้ที่เกี่ยวข้องและมีความจำเป็นต้องใช้ในการปฏิบัติงานจริงทราบและใช้ข้อมูลได้เท่านั้น กรณีที่มีการเปิดเผยข้อมูลต่อบุคคลภายนอกบริษัท จะทำได้ต่อเมื่อได้รับอนุญาตจากหน่วยงานเจ้าของข้อมูลหรือผู้มีอำนาจที่บริษัทฯ กำหนดเท่านั้น

**“ข้อมูลลับ (Confidential)”** หมายถึง ข้อมูลที่มีความสำคัญและมีผลต่อธุรกิจของบริษัทฯ จำกัดสิทธิการเข้าถึงข้อมูลเฉพาะพนักงานหรือผู้ใช้ที่ได้รับมอบหมายเท่านั้น (ส่วนใหญ่เป็นผู้บริหารหรือผู้เกี่ยวข้องโดยตรง) ข้อมูลประเภทนี้จำเป็นต้องเข้ารหัส การเปิดเผยต่อบุคคลภายนอกบริษัทฯ สามารถทำได้ต่อเมื่อได้รับการอนุมัติจากผู้บริหารที่เกี่ยวข้องเท่านั้น โดยมีการกำหนดระดับชั้นความลับไว้เป็น 3 ประเภท ดังนี้

1. **ลับที่สุด** หมายถึง ข้อมูลหรือข่าวสารที่หากมีการเปิดเผยทั้งหมดหรือบางส่วน อาจก่อให้เกิดความเสียหายอย่างร้ายแรงที่สุดต่อบริษัทฯ
2. **ลับมาก** หมายถึง ข้อมูลหรือข่าวสารที่หากมีการเปิดเผยทั้งหมดหรือบางส่วน อาจก่อให้เกิดความเสียหายอย่างร้ายแรงต่อบริษัทฯ
3. **ลับ** หมายถึง ข้อมูลหรือข่าวสารที่หากมีการเปิดเผยทั้งหมดหรือบางส่วน อาจก่อให้เกิดความเสียหายต่อบริษัทฯ

## แนวปฏิบัติเกี่ยวกับชั้นความลับของข้อมูล

### 1. การกำหนดระดับชั้นความลับของข้อมูล

ผู้บริหาร หัวหน้าหน่วยงาน เจ้าของข้อมูล และหน่วยงานเทคโนโลยีสารสนเทศ มีหน้าที่ร่วมกันในการพิจารณาและกำหนดหมวดหมู่ของข้อมูลในระบบสารสนเทศ รวมถึงการกำหนดระดับชั้นความลับของข้อมูลให้เหมาะสมกับลักษณะและความสำคัญของข้อมูลนั้น โดยต้องพิจารณาจากระดับความสำคัญของข้อมูล ความเสี่ยงต่อความมั่นคงปลอดภัย การดำเนินธุรกิจหรือมูลค่าหลักทรัพย์ รวมถึงผลกระทบที่อาจเกิดขึ้นหากข้อมูลถูกเปิดเผย ดัดแปลง สูญหาย หรือถูกเข้าถึงโดยไม่ได้รับอนุญาต และต้องใช้ข้อมูลภายในร่วมกันอย่างสุจริต รอบคอบ ระมัดระวัง

## 2. หลักเกณฑ์การกำหนดชั้นความลับของข้อมูล

การกำหนดชั้นความลับต้องคำนึงถึงระดับความเสี่ยงต่อความมั่นคงปลอดภัยด้านสารสนเทศ ผลกระทบต่อมูลค่าและความเสียหายที่ผู้ใช้บริการ หรือเจ้าของข้อมูลส่วนบุคคลอาจได้รับ ตลอดจนผลกระทบที่อาจเกิดขึ้นต่อทรัพย์สิน ชื่อเสียงทางการค้า และการดำเนินธุรกิจของบริษัทฯ

## 3. อำนาจหน้าที่ในการกำหนดชั้นความลับและการจัดเก็บข้อมูล

ผู้บริหารของเจ้าของข้อมูล (Data Owner) มีอำนาจและหน้าที่ในการกำหนดชั้นความลับและอายุการจัดเก็บข้อมูล โดยต้องดำเนินการให้สอดคล้องกับนโยบายการรักษาความมั่นคงปลอดภัยสารสนเทศ และคำชี้แจงการคุ้มครองข้อมูลส่วนบุคคลของบริษัทฯ อย่างเคร่งครัด ทั้งนี้ ผู้บริหารสามารถมอบหมายให้หัวหน้าหน่วยงานปฏิบัติหน้าที่แทนได้ตามความเหมาะสม และในกรณีเร่งด่วนหัวหน้าหน่วยงานที่ได้รับมอบหมายมีอำนาจกำหนดชั้นความลับชั่วคราวได้

## 4. การจัดเก็บข้อมูลที่มีหลายระดับชั้นความลับ

ในกรณีที่มีการจัดเก็บข้อมูลหลายระดับชั้นความลับรวมกัน (เช่น ภายในโพลเดอร์ย่อยเดียวกัน) ให้ถือปฏิบัติตามระดับชั้นความลับที่สูงที่สุด ผู้จัดการฝ่ายต้องใช้ความรอบคอบสูงสุดเพื่อป้องกันมิให้ข้อมูลที่มีระดับความลับสูงกว่ารั่วไหลออกไป

## 5. การควบคุมการเข้าถึงข้อมูล (Access Control)

ข้อมูลทุกประเภทต้องถูกควบคุมการเข้าถึงตามหลัก “จำเป็นต้องรู้ (Need-to-Know Basis)” โดยอนุญาตเฉพาะบุคลากรที่มีหน้าที่เกี่ยวข้องกับข้อมูลนั้นเท่านั้น สำหรับข้อมูลในระบบสารสนเทศ หากมีการแก้ไขหรือเปลี่ยนแปลงสิทธิ์การเข้าถึงข้อมูล ต้องยื่นคำร้องและได้รับการอนุมัติจากผู้จัดการฝ่ายขึ้นไปผ่านระบบ IT ของบริษัทฯ ก่อนดำเนินการ และเมื่อได้รับการอนุมัติแล้ว ส่วนเทคโนโลยีสารสนเทศจะเป็นผู้กำหนดสิทธิ์การเข้าถึงตามที่ได้รับอนุมัติ

## 6. การเปลี่ยนแปลงระดับชั้นความลับของข้อมูล

การปรับเปลี่ยนระดับชั้นความลับของข้อมูล ไม่ว่าจะเป็นการปรับเพิ่ม ปรับลด หรือยกเลิก ต้องมีเหตุผลและความจำเป็นที่ชัดเจน โดยเฉพาะในกรณีการลดระดับชั้นของข้อมูล ต้องมีการบันทึกเหตุผลประกอบทุกครั้ง

## 7. การจัดเก็บและป้องกันข้อมูล (Data Protection & Storage)

ข้อมูลที่มีระดับชั้นความลับสูง ต้องจัดเก็บในพื้นที่ที่มีการควบคุมพิเศษ เช่น ตู้เอกสารที่ล็อกได้ หรือระบบสารสนเทศที่มีการเข้ารหัสและจำกัดสิทธิ์เข้าถึง ห้ามส่งต่อข้อมูลผ่านช่องทางที่ไม่มีความปลอดภัย เช่น อีเมลส่วนบุคคล หรือแอปพลิเคชันที่ไม่ได้รับอนุญาตจากบริษัทฯ

## 8. การทำลายหรือยกเลิกข้อมูล (Disposal)

เมื่อข้อมูลหมดความจำเป็นในการใช้งาน ต้องดำเนินการทำลายข้อมูลอย่างเหมาะสมตามระดับชั้นความลับ เช่น การทำลายเอกสารด้วยเครื่องทำลายเอกสาร หรือการลบข้อมูลทางอิเล็กทรอนิกส์อย่างถาวรโดยไม่สามารถกู้คืนได้

## 9. การอบรมและสร้างความตระหนักรู้ (Training & Awareness)

บริษัทฯ จะจัดให้มีการอบรมและสื่อสารแนวทางการรักษาความลับของข้อมูลแก่พนักงานอย่างสม่ำเสมอ เพื่อสร้างความเข้าใจและส่งเสริมให้พนักงานทุกระดับตระหนักถึงความสำคัญของการรักษาความปลอดภัยของข้อมูล

## 10. การแจ้งเบาะแส

พนักงานหรือบุคคลใดที่พบเห็นหรือทราบถึงการกระทำที่อาจเข้าข่ายเป็นการละเมิดนโยบายฉบับนี้ สามารถร้องเรียนหรือแจ้งเบาะแสดต่อบริษัทฯ ได้ โดยให้เป็นไปตามขั้นตอนที่กำหนดไว้ในนโยบายการแจ้งเบาะแสดการกระทำผิดของบริษัทฯ ทั้งนี้ บริษัทฯ จะให้ความคุ้มครองแก่ผู้ร้องเรียนหรือผู้แจ้งเบาะแสด โดยข้อมูลและตัวตนของผู้ร้องเรียนจะถูกเก็บรักษาเป็นความลับ และการร้องเรียนดังกล่าวจะไม่มีผลกระทบต่อสถานะการจ้างงาน ตำแหน่ง หรือค่าตอบแทนของผู้ร้องเรียน ทั้งในระหว่างกระบวนการสอบสวนและภายหลังการดำเนินการเสร็จสิ้น

## 11. บทลงโทษ

นโยบายและแนวปฏิบัติเกี่ยวกับชั้นความลับของข้อมูลถือเป็นส่วนหนึ่งของวินัยในการปฏิบัติงานของบริษัทฯ กรรมการ ผู้บริหาร และพนักงานทุกคนต้องปฏิบัติตามนโยบายฉบับนี้อย่างเคร่งครัด หากฝ่าฝืนหรือไม่ปฏิบัติตาม บริษัทฯ จะดำเนินการสอบสวนและพิจารณาลงโทษทางวินัยตามระเบียบข้อบังคับของบริษัทฯ กฎบัตร และกฎหมายที่เกี่ยวข้อง ซึ่งอาจรวมถึงการเลิกจ้างได้ ทั้งนี้ ในกรณีที่มีการสอบสวน พนักงานทุกคนต้องให้ความร่วมมือกับหน่วยงานที่เกี่ยวข้องทั้งภายในและภายนอกบริษัทฯ อย่างเต็มที่

นโยบายและแนวปฏิบัติเกี่ยวกับชั้นความลับของข้อมูล มีผลใช้บังคับตั้งแต่วันที่ 14 พฤศจิกายน 2568 โดยการอนุมัติของคณะกรรมการบริษัท ครั้งที่ 4/2568



---

(นายประธาน ต้นประเสริฐ)

ประธานกรรมการบริษัท

บริษัท ปิ่นทอง อินดัสเตรียล พาร์ค จำกัด (มหาชน)