นโยบายการบริหารจัดการข้อมูลสารสนเทศภายในของบริษัท

บริษัท โปร อินไซด์ จำกัด (มหาชน)

นโยบายการบริหารจัดการข้อมูลสารสนเทศภายในของบริษัทฉบับนี้ จัดทำขึ้นเพื่อกำหนดแนวทางปฏิบัติและมาตรฐานสำหรับ การใช้ การจัดเก็บ และการปกป้องข้อมูลสารสนเทศ ซึ่งเป็นข้อมูลภายในองค์กร อันประกอบไปด้วยข้อมูลทางธุรกิจ ข้อมูลส่วนบุคคลของพนักงาน ตลอดจนข้อมูลที่เป็นทรัพย์สินทางปัญญา และข้อมูลใด ๆ ที่เกี่ยวข้องกับการดำเนินงานของบริษัท (รวมเรียกว่า “ข้อมูล” หรือ “ข้อมูลสารสนเทศ”) โดยมีเป้าหมายในการป้องกันการเข้าถึงข้อมูลดังกล่าวของบริษัทโดยมิชอบ หรือโดยไม่มีอำนาจ รวมทั้งการใช้งานข้อมูลในทางที่ไม่เหมาะสม ตลอดจนส่งเสริมให้พนักงาน และบุคคลที่เกี่ยวข้องทุกคน ใช้งานข้อมูลภายในของบริษัท ด้วยความรับผิดชอบและปฏิบัติตามหลักเกณฑ์ที่กำหนดไว้อย่างเคร่งครัด

1. วัตถุประสงค์และขอบเขต

นโยบายการบริหารจัดการข้อมูลสารสนเทศภายในของบริษัท โปร อินไซด์ จำกัด (มหาชน) (“บริษัท”) ฉบับนี้ จัดทำขึ้นเพื่อส่งเสริมการใช้ข้อมูลภายในอย่างถูกต้อง เหมาะสม และมีประสิทธิภาพ รวมถึงรักษาความมั่นคงปลอดภัยของข้อมูลสำคัญขององค์กร โดยมุ่งเน้นให้การดำเนินงานที่เกี่ยวข้องกับข้อมูลเป็นไปอย่างต่อเนื่อง ป้องกันปัญหาที่อาจเกิดจากการเข้าถึงหรือการใช้งานข้อมูลโดยไม่ได้รับอนุญาต รวมถึงการใช้งานในลักษณะที่ไม่เหมาะสม

นโยบายนี้ยังครอบคลุมถึงการป้องกันภัยคุกคามในทุกรูปแบบที่อาจส่งผลกระทบต่อการดำเนินธุรกิจ และช่วยลดความเสี่ยงที่อาจเกิดขึ้นในอนาคต โดยบริษัทได้กำหนดมาตรฐาน (Standard) แนวปฏิบัติ (Guideline) และขั้นตอนปฏิบัติ (Procedure) ที่ครอบคลุมและสอดคล้องกับแนวทางการรักษาความปลอดภัยของข้อมูล เพื่อสร้างความเชื่อมั่นและความปลอดภัยในการบริหารจัดการข้อมูลภายในองค์กรอย่างมีประสิทธิภาพ ทั้งนี้กำหนดให้มีการทบทวนนโยบายฉบับนี้อย่างน้อยปีละหนึ่งครั้ง หรือกรณีมีเหตุอันสมควร

2. การแบ่งระดับข้อมูล

เพื่อให้การจัดการข้อมูลในองค์กรเป็นไปอย่างเหมาะสมและปลอดภัย บริษัทได้กำหนดระดับของข้อมูลตามความสำคัญและความอ่อนไหว ดังนี้:

2.1 ข้อมูลทั่วไป (Public)

ข้อมูลทั่วไป (Public) ของบริษัท หมายถึง ข้อมูลที่สามารถเผยแพร่หรือเปิดเผยต่อสาธารณชนได้โดยไม่มีข้อจำกัด และไม่ส่งผลกระทบต่อความปลอดภัย การดำเนินงาน หรือชื่อเสียงของบริษัท ข้อมูลในกลุ่มนี้ได้รับการพิจารณาแล้วว่าไม่มีความอ่อนไหว หรือผลกระทบ และสามารถนำไปใช้เพื่อการสื่อสารหรือประชาสัมพันธ์ได้โดยเสรี

ตัวอย่างของข้อมูลทั่วไป (Public):

- ข้อมูลเกี่ยวกับบริษัท เช่น ประวัติบริษัทและวิสัยทัศน์
- รายงานประจำปีที่เปิดเผยต่อสาธารณะ
- ข่าวประชาสัมพันธ์และประกาศต่าง ๆ
- รายละเอียดผลิตภัณฑ์และบริการที่เผยแพร่บนเว็บไซต์
- ข้อมูลที่เกี่ยวข้องกับกิจกรรมเพื่อสังคม

PRO INSIDE PUBLIC COMPANY LIMITED
No.55, A.A.Capital Ratchada Building, 5 Floor,
Ratchadapisek Road, Dindaeng, Dindaeng, Bangkok 10400

บริษัท โปร อินไซด์ จำกัด (มหาชน)
เลขที่ 55 อาคารเอ.เอ.แคปปิตอล รัชดา ชั้นที่ 5 ถนนรัชดาภิเษก
แขวงดินแดง เขตดินแดง กรุงเทพมหานคร 10400
เลขประจำตัวผู้เสียภาษี 0107567000023

Tel : +66 2029 7875
Fax: +66 2029 7879

ข้อมูลประเภทนี้ไม่มีความจำเป็นต้องมีการควบคุมการเข้าถึงอย่างเข้มงวด แต่จะต้องมีความถูกต้องและผ่านการอนุมัติให้เผยแพร่โดยผู้มีอำนาจก่อนเสมอ เพื่อป้องกันความผิดพลาดในการสื่อสารข้อมูลของบริษัทต่อสาธารณะ

2.2 ข้อมูลภายใน (Internal Use Only)

ข้อมูลภายใน (Internal Use Only) ของบริษัท หมายถึง ข้อมูลที่ถูกจำกัดการเข้าถึงและการใช้งานเฉพาะภายในองค์กรเท่านั้น ไม่สามารถเปิดเผยหรือเผยแพร่ให้บุคคลภายนอกทราบได้ เว้นแต่ได้รับการอนุมัติอย่างเป็นทางการจากผู้มีอำนาจ ข้อมูลประเภทนี้อาจเกี่ยวข้องกับการดำเนินงานภายใน นโยบาย หรือแนวปฏิบัติของบริษัทที่หากเปิดเผยอาจส่งผลกระทบต่อความเป็นส่วนตัวหรือการดำเนินธุรกิจของบริษัท

ตัวอย่างของข้อมูลภายใน (Internal Use Only):

- นโยบายและระเบียบปฏิบัติภายในบริษัท
- คู่มือการปฏิบัติงานหรือคู่มือพนักงาน
- ข้อมูลเกี่ยวกับการประชุมภายใน เช่น ระเบียบวาระและบันทึกการประชุม
- รายงานผลการดำเนินงานของแผนกหรือทีมงาน
- ตารางการอบรมหรือกิจกรรมภายใน

ข้อมูลภายในต้องได้รับการจัดการด้วยความระมัดระวัง โดยพนักงานและบุคคลที่เกี่ยวข้องต้องปฏิบัติตามข้อกำหนดและมาตรการที่กำหนดไว้ เพื่อป้องกันการรั่วไหลและการใช้งานโดยไม่ได้รับอนุญาต

2.3 ข้อมูลลับ (Confidential)

ข้อมูลลับ (Confidential) ของบริษัท หมายถึง ข้อมูลที่มีความสำคัญและอ่อนไหวต่อการดำเนินธุรกิจของบริษัท ซึ่งจำเป็นต้องได้รับการปกป้องและจำกัดการเข้าถึงเฉพาะบุคคลที่ได้รับอนุญาตเท่านั้น การเปิดเผยหรือใช้งานข้อมูลดังกล่าวโดยไม่ได้รับอนุญาต อาจก่อให้เกิดผลกระทบเชิงลบต่อองค์กร เช่น ความเสียหายต่อชื่อเสียง ข้อได้เปรียบทางธุรกิจ หรือการละเมิดข้อบังคับทางกฎหมาย

ตัวอย่างของข้อมูลลับ (Confidential):

- ข้อมูลทางการเงิน เช่น งบกำไรขาดทุน รายงานการตรวจสอบบัญชี
- ข้อมูลเกี่ยวกับพนักงาน เช่น เงินเดือนและประวัติการทำงาน
- แผนกลยุทธ์ธุรกิจและโครงการในอนาคต
- ข้อมูลทางการตลาด เช่น แผนส่งเสริมการขายหรือกลยุทธ์การเจาะตลาด
- ข้อตกลงหรือสัญญาที่มีผลผูกพันกับคู่ค้าและพันธมิตรทางธุรกิจ

การจัดการข้อมูลลับต้องมีมาตรการป้องกันที่เหมาะสม เช่น การเข้ารหัส การกำหนดสิทธิ์การเข้าถึง และการกำหนดขั้นตอนในการอนุญาตให้เข้าถึงข้อมูล เพื่อรักษาความปลอดภัยและความเชื่อมั่นในกระบวนการดำเนินธุรกิจของบริษัท

PRO INSIDE PUBLIC COMPANY LIMITED
No.55, A.A.Capital Ratchada Building, 5 Floor,
Ratchadapisek Road, Dindaeng, Dindaeng, Bangkok 10400

บริษัท โปร อินไซด์ จำกัด (มหาชน)
เลขที่ 55 อาคารเอ.เอ.แคปปิตอล รัชดา ชั้นที่ 5 ถนนรัชดาภิเษก
แขวงดินแดง เขตดินแดง กรุงเทพมหานคร 10400
เลขประจำตัวผู้เสียภาษี 0107567000023

Tel : +66 2029 7875
Fax: +66 2029 7879

2.4 ข้อมูลลับเฉพาะบุคคล (Restricted Personal Data)

ข้อมูลลับเฉพาะบุคคล **(Restricted Personal Data)** ของบริษัท หมายถึง ข้อมูลที่มีความสำคัญสูงต่อบุคคลากรขององค์กรโดยตรง เป็นข้อมูลที่มีความอ่อนไหว ข้อมูลส่วนบุคคลที่อาจก่อให้เกิดความเสียหายต่อบุคคลหากถูกเปิดเผย ข้อมูลที่ต้องปฏิบัติตามกฎหมายคุ้มครองข้อมูลส่วนบุคคล เช่น GDPR, PDPA

ตัวอย่างของข้อมูลลับเฉพาะบุคคล

- ข้อมูลบัตรประชาชน, หนังสือเดินทาง
- ข้อมูลสุขภาพและประวัติทางการแพทย์
- ข้อมูลทางการเงินของบุคคล เช่น หมายเลขบัญชีธนาคาร
- ประวัติอาชญากรรม หรือข้อมูลด้านความปลอดภัยของบุคคล

การปกป้องข้อมูลลับเฉพาะบุคคล:

- ใช้การเข้ารหัสข้อมูลแบบเข้มงวด (Encryption)
- กำหนดสิทธิ์การเข้าถึงเฉพาะผู้ที่ได้รับอนุญาตเท่านั้น
- ปฏิบัติตามกฎหมายความเป็นส่วนตัว เช่น PDPA, GDPR
- ห้ามเก็บหรือส่งข้อมูลผ่านช่องทางที่ไม่มีความปลอดภัย

2.5 ข้อมูลลับพิเศษ (Highly Confidential)

ข้อมูลลับพิเศษ (Highly Confidential) ของบริษัท หมายถึง ข้อมูลที่มีความสำคัญสูงสุดต่อการดำเนินธุรกิจหรือความก้าวหน้าขององค์กร ซึ่งต้องได้รับการปกป้องอย่างเข้มงวดและจำกัดการเข้าถึงเฉพาะบุคคลที่ได้รับอนุญาตในระดับสูงสุดเท่านั้น การรั่วไหลหรือการเปิดเผยข้อมูลประเภทนี้อาจก่อให้เกิดความเสียหายร้ายแรงต่อบริษัททั้งในแง่ของการเงิน ชื่อเสียง หรือความได้เปรียบทางการแข่งขัน

ตัวอย่างของข้อมูลลับพิเศษ (Highly Confidential):

- แผนการควบรวมกิจการ หรือแผนการการเข้าซื้อกิจการ
- ข้อมูลทรัพย์สินทางปัญญา เช่น สูตรผลิตภัณฑ์หรือสิทธิบัตรที่อยู่ระหว่างการพัฒนา
- ข้อมูลลูกค้ารายสำคัญหรือความลับทางการค้าของคู่ค้า
- ข้อมูลเกี่ยวกับการฟ้องร้องหรือข้อพิพาททางกฎหมายที่ยังไม่เปิดเผย
- รายละเอียดเกี่ยวกับโครงการสำคัญ

การปกป้องข้อมูลลับพิเศษ:

- ต้องจัดเก็บในระบบที่มีการรักษาความปลอดภัยสูง เช่น การเข้ารหัสหรือการใช้ระบบควบคุมการเข้าถึงที่ซับซ้อน
- มีการกำหนดสิทธิ์การเข้าถึงอย่างเข้มงวด เฉพาะผู้ที่มีความจำเป็นในการใช้งานข้อมูลเท่านั้น
- การถ่ายโอนหรือเผยแพร่ข้อมูลต้องดำเนินการผ่านช่องทางที่ได้รับการอนุมัติและมีการบันทึกการดำเนินการทุกครั้ง
- มีการกำหนดมาตรการปกป้องข้อมูลเชิงพื้นที่ที่เข้าถึง

PRO INSIDE PUBLIC COMPANY LIMITED
No.55, A.A.Capital Ratchada Building, 5 Floor,
Ratchadapisek Road, Dindaeng, Dindaeng, Bangkok 10400

บริษัท โปร อินไซด์ จำกัด (มหาชน)
เลขที่ 55 อาคารเอ.เอ.แคปปิตอล รัชดา ชั้นที่ 5 ถนนรัชดาภิเษก
แขวงดินแดง เขตดินแดง กรุงเทพมหานคร 10400
เลขประจำตัวผู้เสียภาษี 0107567000023

Tel : +66 2029 7875
Fax: +66 2029 7879

ข้อมูลลับพิเศษต้องได้รับการจัดการด้วยความระมัดระวังสูงสุด เพื่อป้องกันความเสี่ยงที่อาจเกิดขึ้นและเพื่อรักษาความมั่นคงปลอดภัยในทุกกระบวนการดำเนินงานของบริษัท การจัดระดับข้อมูลดังกล่าวช่วยให้การใช้งานและการปกป้องข้อมูลในองค์กรเป็นไปอย่างมีประสิทธิภาพและลดความเสี่ยงจากการเข้าถึงหรือการใช้งานที่ไม่เหมาะสม

การยกเลิกการจัดประเภทและการลดระดับความสำคัญของข้อมูลซึ่งถูกจัดอยู่ในประเภท “ข้อมูลลับ” และ “ข้อมูลลับพิเศษ” นั้น ต้องมีการระบุชัดเจนเป็นลายลักษณ์อักษรโดยได้รับการอนุมัติจากผู้ที่มีอำนาจ และแจ้งให้บุคคลที่เกี่ยวข้องทราบ

3. แนวทางการใช้ข้อมูล

3.1 การใช้ข้อมูลเพื่อวัตถุประสงค์ที่ได้รับมอบหมาย

- **การใช้งานข้อมูล**: ข้อมูลสารสนเทศขององค์กรต้องถูกใช้เพื่อสนับสนุนการดำเนินงานหรือการทำงานตามหน้าที่ที่ได้รับมอบหมายเท่านั้น พนักงานต้องใช้ข้อมูลเพื่อช่วยในการตัดสินใจ การวิเคราะห์ หรือการจัดการภายในองค์กรตามนโยบายและขั้นตอนที่กำหนด
- **ห้ามใช้ข้อมูลเพื่อประโยชน์ส่วนตัว**: พนักงานห้ามใช้ข้อมูลในลักษณะที่เกี่ยวข้อง หรือมีวัตถุประสงค์เป็นไปเพื่อประโยชน์ส่วนตัว เช่น การใช้ข้อมูลลูกค้าหรือข้อมูลทางการเงินในการดำเนินการส่วนตัว หรือการให้ข้อมูลแก่บุคคลภายนอกเพื่อประโยชน์ส่วนบุคคลหรือทางการค้า
- **ห้ามใช้ข้อมูลเพื่อประโยชน์บุคคลอื่นที่ไม่เกี่ยวข้อง**: พนักงานต้องไม่แบ่งปันข้อมูลภายในองค์กรให้แก่บุคคลภายนอกใด ๆ ที่ไม่ได้รับอนุญาตให้เข้าถึงหรือล่วงรู้ข้อมูลของบริษัท เช่น การให้ข้อมูลทางการค้าแก่คู่แข่ง หรือการแชร์ข้อมูลที่เกี่ยวข้องกับแผนกลยุทธ์ของบริษัท

3.2 การเข้าถึงข้อมูลผ่านอุปกรณ์และช่องทางที่ปลอดภัย

- **การเข้าถึงข้อมูล**: พนักงานต้องเข้าถึงข้อมูลผ่านอุปกรณ์ที่ได้รับการอนุมัติ ซึ่งกำหนดให้มีรหัสผ่าน (password) หรือมีการเข้ารหัสเพื่อใช้งานอุปกรณ์ที่บรรจุข้อมูลสารสนเทศของบริษัทดังกล่าว อันเป็นมาตรการเพื่อรักษาความมั่นคงปลอดภัยของข้อมูลในองค์กรให้มีประสิทธิภาพสูงขึ้น โดยลดโอกาสของการเข้าถึงโดยไม่ได้รับอนุญาตและป้องกันความเสี่ยงที่อาจส่งผลกระทบต่อธุรกิจ ทั้งนี้จะต้องใช้ความระมัดระวังเป็นพิเศษในกรณีจำเป็นต้องใช้งานอุปกรณ์ดังกล่าวนอกสถานประกอบการด้วย นอกจากนี้แล้วการเข้าถึงข้อมูลต้องกระทำผ่านช่องทางที่ปลอดภัย ประกอบด้วย:
  - **VPN (Virtual Private Network)**: การใช้ VPN จะช่วยให้การเชื่อมต่อจากระยะไกลเป็นไปอย่างปลอดภัย โดยการเข้ารหัสข้อมูลทำให้มั่นใจได้ว่าข้อมูลที่ส่งผ่านเครือข่ายจะไม่ถูกดักจับหรือถูกโจมตี
  - **Multi-Factor Authentication (MFA)**: การใช้ระบบยืนยันตัวตนหลายขั้นตอน (MFA) ช่วยเพิ่มความมั่นคงปลอดภัยในการเข้าถึงข้อมูล โดยต้องมีการยืนยันตัวตนจากหลายแหล่ง เช่น รหัสผ่านและรหัส OTP ที่ส่งไปยังโทรศัพท์มือถือหรืออีเมล
  - **การเข้าถึงผ่านระบบที่ได้รับการอนุมัติ**: ทุกการเข้าถึงข้อมูลต้องผ่านระบบที่มีการควบคุมและบันทึกการใช้งาน เช่น ระบบจัดการสิทธิ์การเข้าถึง (Access Management System) ที่จะช่วยจำกัดการเข้าถึงข้อมูลตามระดับความสำคัญของข้อมูล

PRO INSIDE PUBLIC COMPANY LIMITED
No.55, A.A.Capital Ratchada Building, 5 Floor,
Ratchadapisek Road, Dindaeng, Dindaeng, Bangkok 10400

บริษัท โปร อินไซด์ จำกัด (มหาชน)
เลขที่ 55 อาคารเอ.เอ.แคปปิตอล รัชดา ชั้นที่ 5 ถนนรัชดาภิเษก
แขวงดินแดง เขตดินแดง กรุงเทพมหานคร 10400
เลขประจำตัวผู้เสียภาษี 0107567000023

Tel : +66 2029 7875
Fax: +66 2029 7879

3.3 การดัดแปลงหรือแก้ไขข้อมูล

- **ห้ามดัดแปลงข้อมูลโดยไม่ได้รับอนุญาต**: พนักงานห้ามทำการแก้ไขหรือดัดแปลงข้อมูลในระบบขององค์กรโดยไม่ได้รับอนุญาตจากผู้มีอำนาจที่เกี่ยวข้อง เช่น การเปลี่ยนแปลงข้อมูลทางการเงิน ข้อมูลการผลิต หรือข้อมูลลูกค้า
- **การแก้ไขข้อมูลต้องมีการตรวจสอบ**: การปรับเปลี่ยนข้อมูลที่สำคัญต้องมีการตรวจสอบและบันทึกกระบวนการอย่างเป็นทางการ เช่น การใช้ระบบตรวจสอบประวัติการเข้าถึงและการแก้ไขข้อมูล (Audit Trail) ที่สามารถติดตามการเปลี่ยนแปลงที่เกิดขึ้นได้
- **การเผยแพร่ข้อมูลต้องได้รับอนุญาต**: การเผยแพร่ข้อมูลที่เกี่ยวข้องกับธุรกิจหรือข้อมูลที่มีความอ่อนไหวต้องได้รับการอนุมัติจากผู้มีอำนาจ เช่น ข้อมูลลูกค้าหรือข้อมูลทางการเงิน

3.4 การเปิดเผยข้อมูลของบริษัท

- **ห้ามเปิดเผยข้อมูลของบริษัทโดยไม่ได้รับอนุญาต**: ข้อมูลที่ได้รับการจัดระดับความลับหรือข้อมูลที่เกี่ยวข้องกับกิจกรรมหรือกลยุทธ์ทางธุรกิจของบริษัทจะต้องไม่ถูกเปิดเผยให้แก่บุคคลภายนอก หรือใช้ในลักษณะที่อาจส่งผลเสียต่อบริษัท หากต้องการเปิดเผยข้อมูลดังกล่าวจะต้องได้รับอนุญาตจากผู้บริหารหรือบุคคลที่ได้รับมอบหมาย
- **การเปิดเผยข้อมูลต้องสอดคล้องกับนโยบาย**: เปิดเผยข้อมูลสารสนเทศของบริษัทต้องดำเนินการโดยสอดคล้องกับนโยบายการบริหารจัดการข้อมูลสารสนเทศภายในของบริษัทฉบับนี้ ตลอดจนนโยบายหรือหลักปฏิบัติอื่นใดของบริษัทที่เกี่ยวข้อง และตามข้อกำหนดที่กฎหมายกำหนด เช่น การเปิดเผยข้อมูลภายใต้ข้อตกลงทางธุรกิจหรือการให้ข้อมูลแก่หน่วยงานภาครัฐตามคำสั่งศาล

4. การปกป้องข้อมูลเชิงพื้นที่ที่เข้าถึง

การปกป้องข้อมูลในเชิงพื้นที่เป็นมาตรการสำคัญที่ช่วยควบคุมการเข้าถึงข้อมูลของบริษัท โดยการกำหนดพื้นที่ที่สามารถเข้าถึงข้อมูลต่าง ๆ ได้อย่างเหมาะสมและปลอดภัย เพื่อป้องกันการเข้าถึงโดยบุคคลที่ไม่ได้รับอนุญาต และลดความเสี่ยงจากการรั่วไหลหรือการโจรกรรมข้อมูล

4.1 พื้นที่ควบคุมการเข้าถึง (Restricted Areas)

4.1.1 กำหนดโซนพื้นที่ที่มีการเข้าถึงข้อมูลลับ (Confidential) หรือข้อมูลลับสุดยอด (Highly Confidential) เช่น

4.1.1.1 ห้องเซิร์ฟเวอร์: พื้นที่ที่เก็บเซิร์ฟเวอร์หรืออุปกรณ์จัดเก็บข้อมูลสำคัญต้องมีการควบคุมอย่างเข้มงวด เช่น การจำกัดการเข้าใช้เฉพาะเจ้าหน้าที่ที่มีความจำเป็นต้องเข้าไปเท่านั้น

4.1.1.2 ศูนย์ข้อมูล (Data Center): ศูนย์ข้อมูลที่เก็บข้อมูลสำคัญของบริษัทจะต้องมีมาตรการป้องกันหลายชั้น เช่น ระบบควบคุมการเข้าถึง และการรักษาความปลอดภัยทางกายภาพ

4.1.1.3 ห้องประชุมสำคัญ (Executive Rooms): ห้องประชุมที่ใช้สำหรับการประชุมที่เกี่ยวข้องกับข้อมูลที่มีความอ่อนไหว เช่น แผนธุรกิจ กลยุทธ์ หรือการตัดสินใจที่สำคัญต้องมีการจำกัดการเข้าถึงและติดตามการใช้พื้นที่

PRO INSIDE PUBLIC COMPANY LIMITED
No.55, A.A.Capital Ratchada Building, 5 Floor,
Ratchadapisek Road, Dindaeng, Dindaeng, Bangkok 10400

บริษัท โปร อินไซด์ จำกัด (มหาชน)
เลขที่ 55 อาคารเอ.เอ.แคปปิตอล รัชดา ชั้นที่ 5 ถนนรัชดาภิเษก
แขวงดินแดง เขตดินแดง กรุงเทพมหานคร 10400
เลขประจำตัวผู้เสียภาษี 0107567000023

Tel : +66 2029 7875
Fax: +66 2029 7879

4.2 ติดตั้งระบบควบคุมการเข้าถึง

4.2.1 การใช้บัตรผ่านเข้า-ออกประตู (Access Card): ใช้บัตรที่มีระบบการเก็บข้อมูลเพื่อควบคุมการเข้าออกพื้นที่ที่มีข้อมูลสำคัญ พนักงานที่ได้รับอนุญาตสามารถใช้บัตรผ่านเพื่อเข้าถึงพื้นที่ที่มีข้อมูลลับ โดยมีการบันทึกการเข้าออกในระบบ รวมถึงการจัดให้มีพื้นที่ ที่แลกบัตรสำหรับผู้มาติดต่อ

4.2.2 รหัสผ่าน (Password): พื้นที่ที่มีความสำคัญสูงควรกำหนดให้ใช้รหัสผ่านที่มีความปลอดภัยสูง โดยรหัสผ่านต้องมีความยาวและมีความซับซ้อน เพื่อป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต

4.2.3 Face Recognition (การสแกนใบหน้า): ใช้เทคโนโลยีการสแกนใบหน้าสำหรับการตรวจสอบตัวตน ซึ่งเป็นระบบที่มีความแม่นยำสูงและยากที่จะปลอมแปลงการเข้าถึง

4.3 การควบคุมการเข้า-ออกพื้นที่ (Access Control for Restricted Areas)

เพื่อให้การเข้าถึงพื้นที่ที่จัดเก็บหรือดำเนินการเกี่ยวกับข้อมูลลับ (Confidential) และข้อมูลลับพิเศษ (Highly Confidential) มีความปลอดภัยสูงสุด บริษัทได้กำหนดแนวทางและมาตรการควบคุมการเข้า-ออกพื้นที่ดังนี้:

4.3.1 การบันทึกข้อมูลการเข้า-ออกพื้นที่

การบันทึกข้อมูลการเข้า-ออกพื้นที่ที่จัดเก็บข้อมูลสำคัญต้องดำเนินการโดยละเอียดและต่อเนื่อง เพื่อให้สามารถติดตามตรวจสอบย้อนหลังได้ในกรณีที่เกิดเหตุการณ์ผิดปกติ:

4.3.1.1 เวลาเข้า-ออก:

- ระบบจะบันทึกเวลาที่บุคคลเข้าสู่และออกจากพื้นที่โดยอัตโนมัติ เช่น ผ่านเครื่องสแกนบัตรหรือระบบการยืนยันตัวตนทางไบโอเมตริกส์ (Biometric Authentication)

4.3.1.2 ชื่อผู้เข้าใช้งาน:

- ระบุชื่อและตำแหน่งของผู้ที่เข้าพื้นที่เพื่อให้สามารถตรวจสอบตัวตนได้ชัดเจน
- หากเป็นบุคคลภายนอก เช่น ผู้รับเหมา หรือผู้ตรวจสอบ ต้องมีการลงทะเบียนชื่อ-นามสกุล และสังกัดล่วงหน้าก่อนการเข้าถึงพื้นที่

4.3.1.3 เหตุผลในการเข้าถึง:

- ต้องบันทึกวัตถุประสงค์การเข้าถึงอย่างชัดเจน เช่น การตรวจสอบอุปกรณ์ การประชุม หรือการเข้าถึงข้อมูลเฉพาะทาง
- บุคคลที่ไม่ได้แจ้งเหตุผลล่วงหน้าจะไม่ได้รับอนุญาตให้เข้าสู่พื้นที่

4.3.2 การเข้าถึงของบุคคลภายนอก

การเข้าถึงพื้นที่ที่มีข้อมูลสำคัญโดยบุคคลภายนอก เช่น ผู้ตรวจสอบ หรือคู่ค้าธุรกิจ ต้องเป็นไปตามขั้นตอนที่เคร่งครัด ดังนี้:

4.3.2.1 การแจ้งเตือนล่วงหน้า:

- บุคคลภายนอกต้องส่งคำขอเข้าถึงพื้นที่ล่วงหน้าพร้อมแจ้งวัตถุประสงค์ ระบุระยะเวลา และผู้ที่ต้องรับผิดชอบในการดูแล

PRO INSIDE PUBLIC COMPANY LIMITED
No.55, A.A.Capital Ratchada Building, 5 Floor,
Ratchadapisek Road, Dindaeng, Dindaeng, Bangkok 10400

บริษัท โปร อินไซด์ จำกัด (มหาชน)
เลขที่ 55 อาคารเอ.เอ.แคปปิตอล รัชดา ชั้นที่ 5 ถนนรัชดาภิเษก
แขวงดินแดง เขตดินแดง กรุงเทพมหานคร 10400
เลขประจำตัวผู้เสียภาษี 0107567000023

Tel : +66 2029 7875
Fax: +66 2029 7879

4.3.2.2 การอนุมัติจากผู้มีอำนาจ:

- ต้องได้รับอนุมัติจากเจ้าหน้าที่ที่เกี่ยวข้อง ผู้จัดการฝ่ายที่เกี่ยวข้อง หรือผู้บริหารที่ได้รับมอบหมาย โดยพิจารณาความจำเป็นและความเหมาะสม

4.3.2.3 การดูแลระหว่างการเข้าถึง:

- บุคคลภายนอกจะต้องมีเจ้าหน้าที่ของบริษัทคอยดูแลตลอดเวลา
- ห้ามบุคคลภายนอกเข้าใช้หรือเข้าถึงอุปกรณ์หรือข้อมูลโดยไม่มีการควบคุม

4.3.3 การตรวจสอบและบันทึกข้อมูล

มาตรการตรวจสอบและจัดเก็บบันทึกข้อมูลการเข้า-ออกพื้นที่ช่วยเสริมสร้างความมั่นคงและลดความเสี่ยงจากการเข้าถึงที่ไม่เหมาะสม:

4.3.3.1 ระบบตรวจสอบการเข้าถึง (Access Monitoring System):

- พื้นที่ที่จัดเก็บข้อมูลลับต้องติดตั้งระบบตรวจสอบการเข้า-ออก เช่น กล้องวงจรปิด (CCTV) และระบบบันทึกข้อมูลการเข้าถึง
- มีการตรวจสอบประวัติการเข้า-ออกอย่างสม่ำเสมอ เช่น รายสัปดาห์หรือรายเดือน เพื่อระบุความผิดปกติ

4.3.3.2 การจัดเก็บบันทึกการเข้า-ออก:

- ข้อมูลการเข้า-ออกพื้นที่ควรเก็บรักษาในระบบที่ปลอดภัยและเข้าถึงได้เฉพาะผู้มีอำนาจ เช่น การใช้ระบบจัดการสิทธิ์การเข้าถึง (Access Rights Management System)
- บันทึกข้อมูลการเข้า-ออก จะถูกจัดเก็บไว้เป็นระยะเวลาตามความเหมาะสมและความจำเป็นด้านความปลอดภัย แต่ทั้งนี้ไม่เกิน 1 ปี เพื่อใช้ในการตรวจสอบหรือสอบสวนหากเกิดเหตุการณ์ไม่พึงประสงค์

4.3.4 การแจ้งเตือนและดำเนินการในกรณีผิดปกติ

4.3.4.1 การแจ้งเตือนอัตโนมัติ:

- หากพบการพยายามเข้าถึงพื้นที่โดยไม่ได้รับอนุญาต ระบบจะส่งการแจ้งเตือนไปยังผู้ดูแลความปลอดภัยหรือผู้จัดการฝ่ายที่เกี่ยวข้องทันที

4.3.4.2 การตรวจสอบความผิดปกติ:

- เจ้าหน้าที่ความปลอดภัย (Physical Security) จะต้องตรวจสอบเหตุการณ์และดำเนินการตามขั้นตอนที่กำหนด เช่น การตรวจสอบกล้องวงจรปิด การยืนยันตัวบุคคล และการรายงานผู้บริหาร

มาตรการเหล่านี้มีเป้าหมายเพื่อป้องกันการเข้าถึงพื้นที่สำคัญโดยไม่ได้รับอนุญาต ควบคุมความเสี่ยงในการรั่วไหลหรือการโจมตีข้อมูล และรักษาความปลอดภัยของข้อมูลที่สำคัญต่อการดำเนินธุรกิจ

PRO INSIDE PUBLIC COMPANY LIMITED
No.55, A.A.Capital Ratchada Building, 5 Floor,
Ratchadapisek Road, Dindaeng, Dindaeng, Bangkok 10400

บริษัท โปร อินไซด์ จำกัด (มหาชน)
เลขที่ 55 อาคารเอ.เอ.แคปปิตอล รัชดา ชั้นที่ 5 ถนนรัชดาภิเษก
แขวงดินแดง เขตดินแดง กรุงเทพมหานคร 10400
เลขประจำตัวผู้เสียภาษี 0107567000023

Tel : +66 2029 7875
Fax: +66 2029 7879

4.4 กำหนดให้มีการเข้ารหัสสำหรับอุปกรณ์จัดเก็บข้อมูลสารสนเทศ

การกำหนดให้มีรหัสผ่าน (password) หรือมีการเข้ารหัสเพื่อใช้งานอุปกรณ์ที่บรรจุข้อมูลสารสนเทศของบริษัท เป็นมาตรการสำหรับรักษาความปลอดภัยของข้อมูลในองค์กรให้มีประสิทธิภาพสูงขึ้น โดยลดโอกาสของการเข้าถึงโดยไม่ได้รับอนุญาตและป้องกันความเสี่ยงที่อาจส่งผลกระทบต่อธุรกิจ นอกจากนั้น จะต้องใช้ความระมัดระวังเป็นพิเศษหากจำเป็นต้องใช้งานอุปกรณ์ดังกล่าวนอกสถานประกอบการด้วย

5. การเข้าถึงและการจำกัดสิทธิ์ (Access Control)

การจัดการสิทธิ์ในการเข้าถึงข้อมูลของพนักงานและบุคคลที่เกี่ยวข้องในบริษัท เป็นปัจจัยสำคัญในการรักษาความปลอดภัยของข้อมูล และป้องกันการใช้ข้อมูลในทางที่ไม่เหมาะสม โดยบริษัทได้กำหนดแนวทางดังนี้:

5.1 การกำหนดสิทธิ์การเข้าถึงข้อมูลตามบทบาทและหน้าที่

5.1.1 การกำหนดสิทธิ์ตามระดับของพนักงาน:

5.1.1.1 พนักงานแต่ละคนจะได้รับสิทธิ์ในการเข้าถึงข้อมูลที่เหมาะสมกับระดับงานและความจำเป็นในการปฏิบัติงานเท่านั้น เช่น ระบบงาน Orbit

- พนักงานระดับผู้จัดการขึ้นไป สามารถเข้าถึงข้อมูลที่เกี่ยวข้องกับการบริหารจัดการ
- พนักงานทั่วไปสามารถเข้าถึงข้อมูลเฉพาะที่จำเป็นสำหรับการทำงานของตน เช่น การลงเวลาเข้า - ออก

5.1.1.2 การกำหนดสิทธิ์เฉพาะตามบทบาทหน้าที่ (Role-Based Access Control - RBAC):

- การกำหนดให้ระบบงานสามารถจำแนกสิทธิ์การเข้าถึงข้อมูล ตามบทบาทหน้าที่ หรือเจ้าหน้าที่เฉพาะหน่วยงานที่เกี่ยวข้อง เช่น ฝ่ายการเงิน ฝ่ายทรัพยากรบุคคล หรือฝ่ายไอที เพื่อป้องกันการเข้าถึงข้อมูลที่ไม่เกี่ยวข้อง

5.1.2 การสื่อสารและการอบรมด้านการรักษาความปลอดภัยของข้อมูล

5.1.2.1 พนักงานใหม่:

- ก่อนเริ่มปฏิบัติงาน พนักงานใหม่ทุกคนต้องเข้าร่วมการฝึกอบรมด้านการรักษาความปลอดภัยของข้อมูล ซึ่งรวมถึง
  - การเรียนรู้เกี่ยวกับนโยบายการรักษาความลับและการปกป้องข้อมูลภายในของบริษัท
  - การป้องกันภัยคุกคามทางไซเบอร์ เช่น ฟิชชิ่ง (Phishing) และมัลแวร์
  - กฎหมายอื่นๆที่เกี่ยวข้อง เช่น พรบ คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 (PDPA)
  - วิธีการเข้าถึงข้อมูลอย่างปลอดภัย เช่น การใช้รหัสผ่านที่ซับซ้อน การยืนยันตัวตนหลายขั้นตอน Multi Factor Autentication (MFA)

PRO INSIDE PUBLIC COMPANY LIMITED
No.55, A.A.Capital Ratchada Building, 5 Floor,
Ratchadapisek Road, Dindaeng, Dindaeng, Bangkok 10400

บริษัท โปร อินไซด์ จำกัด (มหาชน)
เลขที่ 55 อาคารเอ.เอ.แคปปิตอล รัชดา ชั้นที่ 5 ถนนรัชดาภิเษก
แขวงดินแดง เขตดินแดง กรุงเทพมหานคร 10400
เลขประจำตัวผู้เสียภาษี 0107567000023

Tel : +66 2029 7875
Fax: +66 2029 7879

5.1.2.2 บุคคลภายนอก:

- บุคคลภายนอก เช่น ผู้ตรวจสอบ ผู้รับเหมา หรือคู่ค้าธุรกิจ ที่ได้รับสิทธิ์เข้าถึงข้อมูลของบริษัท ซึ่งมิได้เป็นข้อมูลสาธารณะ หรือข้อมูลที่สามารถเปิดเผยได้โดยทั่วไป ต้องมีกระบวนแจ้งให้ทราบถึงข้อกำหนดและเงื่อนไขการเข้าถึงข้อมูลของบริษัท รวมถึงลงนามในสัญญารักษาความลับ Non-disclosure agreement (NDA) ในกรณีที่ต้องเข้าถึงข้อมูลของบริษัทตั้งแต่ชั้นข้อมูลภายในขึ้นไป

5.1.3 การยกเลิกสิทธิ์เมื่อพ้นสภาพการทำงานหรือสิ้นสุดสัญญา

5.1.3.1 การยกเลิกสิทธิ์การเข้าถึงข้อมูลหรือระบบงาน:

- เมื่อพนักงานพ้นจากตำแหน่ง สิ้นสุดสัญญาการจ้างงาน หรือเปลี่ยนแปลงตำแหน่งงาน ฝ่ายทรัพยากรบุคคล (PD) ดำเนินการแจ้งฝ่ายไอทีทันที เพื่อเจ้าหน้าที่ที่เกี่ยวข้องทำการยกเลิกสิทธิ์การเข้าถึงข้อมูล และระบบงานของบริษัท เพื่อป้องกันการใช้งานข้อมูลที่ไม่เหมาะสม

5.1.3.2 การตรวจสอบสิทธิ์เป็นระยะ:

- สิทธิ์การเข้าถึงข้อมูลของพนักงาน หรือบุคคลภายนอกจะต้องได้รับการตรวจสอบเป็นระยะ เช่น ทุก 6 เดือน หรือ เพื่อให้มั่นใจว่าสิทธิ์ที่กำหนดสอดคล้องกับบทบาทหน้าที่ในปัจจุบัน

5.2 . การควบคุมการเข้าถึงข้อมูลสำหรับบุคคลภายนอก

5.2.1 บุคคลภายนอก เช่น ผู้ตรวจสอบ คู่ค้า หรือผู้รับเหมา จะต้องได้รับ อนุมัติเป็นลายลักษณ์อักษร จากผู้มีอำนาจในบริษัทก่อนเข้าถึงข้อมูลใด ๆ

5.2.2 การเข้าถึงข้อมูลจะถูกจำกัดเฉพาะใน ขอบเขตที่จำเป็น ต่อการปฏิบัติงานเท่านั้น โดยกำหนดสิทธิ์เข้าถึงเฉพาะข้อมูลที่เกี่ยวข้อง

5.2.2.1 มีการบันทึกข้อมูลการเข้าถึงของบุคคลภายนอก เช่น:

- ชื่อ-นามสกุล
- ชื่อองค์กร
- เวลาและวันที่เข้า-ออก
- รายละเอียดของข้อมูลหรือระบบที่ได้รับการเข้าถึง
- วัตถุประสงค์ในการเข้าถึง

5.2.2.2 กระบวนการควบคุมการเปิดเผยข้อมูลโดยบุคคลภายนอก

จะต้องมีการควบคุมป้องกันการเปิดเผยข้องมูล หรือการรั่วไหลของข้อมูลที่เหมาะสม เช่น สำหรับการปฏิบัติงานของผู้ตรวจสอบ จะต้องมีการจัดพื้นที่ในการเข้าปฏิบัติงานให้เป็นสัดส่วน มิให้นำเอกสารออกจากพื้นที่ควบคุม จัดให้มีกล้องวงจรปิดบันทึกการปฏิบัติแบบมุมกว้าง ไม่อนุญาตให้นำเครื่องโทรศัพท์ หรืออุปกรณ์บันทึกภาพ เสียงเข้าในพื้นที่ และมีเจ้าหน้าที่ของบริษัทที่ได้รับมอบหมายอยู่ในพื้นที่ ในระหว่างปฏิบัติงาน

5.2.2.3 ติดตามกิจกรรมในระบบอย่างต่อเนื่อง เช่น การดาวน์โหลดหรือการแก้ไขข้อมูล เพื่อป้องกันการกระทำที่ผิดปกติ

PRO INSIDE PUBLIC COMPANY LIMITED
No.55, A.A.Capital Ratchada Building, 5 Floor,
Ratchadapisek Road, Dindaeng, Dindaeng, Bangkok 10400

บริษัท โปร อินไซด์ จำกัด (มหาชน)
เลขที่ 55 อาคารเอ.เอ.แคปปิตอล รัชดา ชั้นที่ 5 ถนนรัชดาภิเษก
แขวงดินแดง เขตดินแดง กรุงเทพมหานคร 10400
เลขประจำตัวผู้เสียภาษี 0107567000023

Tel : +66 2029 7875
Fax: +66 2029 7879

5.2.3 การใช้พื้นที่และอุปกรณ์สำหรับบุคคลภายนอก

บุคคลภายนอกที่ทำงานภายในพื้นที่ของบริษัทจะได้รับอนุญาตให้ใช้งาน เฉพาะอุปกรณ์ที่บริษัทจัดเตรียมให้ เช่น คอมพิวเตอร์หรือเครือข่ายอินเทอร์เน็ต ห้ามใช้เครือข่าย Wi-Fi สาธารณะ หรืออุปกรณ์ส่วนตัว เช่น แฟลชไดรฟ์ หรือโน้ตบุ๊ก ในการเข้าถึงข้อมูลของบริษัท ยกเว้นได้รับอนุมัติจากฝ่ายไอที

5.2.4 การควบคุมข้อมูลที่ส่งมอบให้บุคคลภายนอก

- ข้อมูลที่ส่งมอบให้บุคคลภายนอกต้องได้รับการตรวจสอบและอนุมัติจากผู้มีอำนาจ
- ข้อมูลที่มีความลับ เช่น ข้อมูลลับ (Confidential) หรือข้อมูลลับพิเศษ (Highly Confidential) ต้องผ่านกระบวนการ เข้ารหัส (Encryption) ก่อนส่งมอบ
- ห้ามส่งข้อมูลผ่านช่องทางที่ไม่มีความปลอดภัย เช่น อีเมลส่วนตัว หรือแอปพลิเคชันส่งข้อความที่ไม่ได้รับการรับรอง

6. การรักษาความลับและการป้องกันข้อมูล (Data Protection)

เพื่อปกป้องข้อมูลสำคัญของบริษัท ให้มีความปลอดภัยสูงสุด บริษัทได้กำหนดมาตรการในการรักษาความลับและป้องกันข้อมูล โดยครอบคลุมทั้งข้อมูลดิจิทัลและข้อมูลที่เป็นเอกสารดังนี้:

6.1 การเข้ารหัสข้อมูล (Encryption)

6.1.1 ข้อมูลที่มีความลับ เช่น ข้อมูลลับ (Confidential) และข้อมูลลับสุดยอด (Highly Confidential) จะต้องได้รับการเข้ารหัส ที่มีมาตราฐาน เช่น AES-256 สำหรับข้อมูลดิจิทัล เพื่อป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต

6.2 การจัดการข้อมูลในอุปกรณ์ส่วนตัว

6.2.1 ห้ามพนักงาน บันทึกข้อมูลที่มีความลับลงในอุปกรณ์ส่วนตัว เช่น คอมพิวเตอร์ แล็ปท็อป หรือโทรศัพท์มือถือส่วนตัว ยกเว้นในกรณีที่ได้รับอนุญาตและอุปกรณ์ดังกล่าวมีการติดตั้งระบบรักษาความปลอดภัยที่เหมาะสม

6.2.2 หากจำเป็นต้องใช้ข้อมูลผ่านอุปกรณ์ส่วนตัว ต้องใช้ระบบที่บริษัทกำหนด โดยอ้างอิงตาม นโยบายการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ

6.3 การจัดการข้อมูลที่เป็นเอกสาร

เอกสารที่มีข้อมูลลับต้องจัดเก็บในพื้นที่ที่ปลอดภัย เช่น:

6.3.1 ตู้เก็บเอกสารที่มีการล็อก: ใช้กุญแจหรือระบบล็อกอิเล็กทรอนิกส์

6.3.2 ห้องเก็บเอกสารควบคุม: ซึ่งมีระบบการเข้าถึงเฉพาะบุคคลที่ได้รับอนุญาตเท่านั้น

- ห้ามนำเอกสารที่มีข้อมูลลับออกจากพื้นที่ที่กำหนดโดยไม่ได้รับอนุญาตจากผู้มีอำนาจ
- การกำจัดเอกสารที่ไม่ใช้งานแล้ว:
  - เอกสารที่มีข้อมูลลับต้องถูกทำลายอย่างปลอดภัย เช่น ใช้เครื่องย่อยเอกสาร (Shredder) หรือบริการทำลายเอกสารจากผู้ให้บริการที่ได้รับอนุญาต

PRO INSIDE PUBLIC COMPANY LIMITED
No.55, A.A.Capital Ratchada Building, 5 Floor,
Ratchadapisek Road, Dindaeng, Dindaeng, Bangkok 10400

บริษัท โปร อินไซด์ จำกัด (มหาชน)
เลขที่ 55 อาคารเอ.เอ.แคปปิตอล รัชดา ชั้นที่ 5 ถนนรัชดาภิเษก
แขวงดินแดง เขตดินแดง กรุงเทพมหานคร 10400
เลขประจำตัวผู้เสียภาษี 0107567000023

Tel : +66 2029 7875
Fax: +66 2029 7879

6.4 การป้องกันการเปิดเผยข้อมูลโดยไม่ได้รับอนุญาต

เพื่อป้องกันความเสี่ยงจากการเปิดเผยข้อมูลโดยไม่ได้รับอนุญาต บริษัท ได้กำหนดแนวทางปฏิบัติเพื่อรักษาความลับของข้อมูลที่สำคัญ โดยมีรายละเอียดดังนี้:

6.4.1 ห้ามพนักงานดำเนินการใดที่อาจนำไปสู่การเปิดเผยข้อมูลลับโดยไม่ได้รับอนุญาต

6.4.1.1 การเปิดเผยข้อมูลต่อบุคคลอื่น:

พนักงานไม่มีสิทธิ์เปิดเผยข้อมูลลับ (Confidential) หรือข้อมูลลับพิเศษ (Highly Confidential) ให้แก่บุคคลอื่นที่ไม่มีสิทธิ์เข้าถึงข้อมูลนั้น รวมถึงเพื่อนร่วมงานที่ไม่ได้รับอนุญาต การเปิดเผยข้อมูลจะต้องได้รับอนุมัติเป็นลายลักษณ์อักษรจากผู้บังคับบัญชาหรือเจ้าของข้อมูล

6.4.1.2 การสนทนาในพื้นที่ที่ไม่ปลอดภัย:

ห้ามสนทนาหรือหารือเกี่ยวกับข้อมูลลับในพื้นที่สาธารณะ เช่น โรงอาหาร ลิฟต์ หรือพื้นที่ที่บุคคลที่ไม่เกี่ยวข้องอาจได้ยิน หลีกเลี่ยงการหารือข้อมูลลับในพื้นที่ที่มีการติดตั้งกล้องวงจรปิดหรืออุปกรณ์บันทึกเสียง

6.4.2 การจัดการข้อมูลในระหว่างการประชุมหรือการนำเสนอ

6.4.2.1 การแก้ไขและปกปิดข้อมูลที่สำคัญ:

- ก่อนนำข้อมูลไปใช้ในการประชุม นำเสนอ หรือจัดทำเอกสาร ต้องตรวจสอบว่ามีการแก้ไขหรือปกปิดส่วนที่เป็นข้อมูลลับในกรณีที่ผู้เข้าร่วมไม่มีสิทธิ์เข้าถึง
- ใช้เอกสารที่ระบุชัดเจนถึง ระดับความลับ (เช่น การพิมพ์คำว่า "Confidential" หรือ "Highly Confidential") เพื่อเน้นย้ำความสำคัญของข้อมูล

6.4.2.2 การตรวจสอบผู้เข้าร่วมประชุม:

- การประชุมผ่านช่องทางออนไลน์ จะต้องตรวจสอบรายชื่อผู้เข้าร่วมประชุมเพื่อจำกัดการเข้าถึงข้อมูลให้เฉพาะผู้ที่ได้รับอนุญาตเท่านั้น
- การประชุมที่มีการนำเสนอข้อมูลลับต้องจัดในพื้นที่ปลอดภัย เช่น ห้องประชุมที่ล็อกได้ และไม่มีบุคคลที่ไม่ได้รับอนุญาตอยู่ในบริเวณดังกล่าว

6.4.3 การใช้สื่ออิเล็กทรอนิกส์และอุปกรณ์เพื่อสื่อสารข้อมูล

6.4.3.1 การส่งข้อมูลผ่านสื่ออิเล็กทรอนิกส์:

- ห้ามส่งข้อมูลลับผ่านอีเมลส่วนตัว หรือช่องทางที่ไม่มีการเข้ารหัส เช่น แอปพลิเคชันส่งข้อความที่ไม่มีระบบความปลอดภัย
- หากจำเป็นต้องส่งข้อมูลลับ ต้องใช้ระบบที่มีการเข้ารหัส (Encryption) และมีการยืนยันตัวตนของผู้รับอย่างชัดเจน

PRO INSIDE PUBLIC COMPANY LIMITED
No.55, A.A.Capital Ratchada Building, 5 Floor,
Ratchadapisek Road, Dindaeng, Dindaeng, Bangkok 10400

บริษัท โปร อินไซด์ จำกัด (มหาชน)
เลขที่ 55 อาคารเอ.เอ.แคปปิตอล รัชดา ชั้นที่ 5 ถนนรัชดาภิเษก
แขวงดินแดง เขตดินแดง กรุงเทพมหานคร 10400
เลขประจำตัวผู้เสียภาษี 0107567000023

Tel : +66 2029 7875
Fax: +66 2029 7879

6.4.3.2 การป้องกันการบันทึกข้อมูลโดยไม่ได้รับอนุญาต:

- ห้ามบันทึกข้อมูลลับ หรือข้อมูลลับสุดยอดลงในอุปกรณ์ส่วนตัว เช่น โทรศัพท์มือถือหรือคอมพิวเตอร์ส่วนตัว ยกเว้นในกรณีที่ได้รับอนุญาตจากฝ่ายที่เกี่ยวข้อง
- ในการประชุมออนไลน์ ต้องปิดฟังก์ชันการบันทึกหรือแชร์หน้าจอ ยกเว้นได้รับอนุญาตจากผู้ที่เกี่ยวข้อง

มาตรการเหล่านี้มุ่งเน้นให้บริษัทสามารถป้องกันการรั่วไหลของข้อมูลที่สำคัญ ลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ และสร้างความเชื่อมั่นให้กับพนักงาน คู่ค้า และลูกค้าในการปฏิบัติงานอย่างปลอดภัยและเป็นมืออาชีพ

7. การติดตามและการตรวจสอบ (Monitoring and Audit)

เพื่อให้มั่นใจว่าการใช้งานข้อมูลภายในบริษัทเป็นไปตามนโยบายที่กำหนด และเพื่อป้องกันเหตุการณ์ที่อาจส่งผลกระทบต่อความปลอดภัยของข้อมูล บริษัทได้กำหนดแนวทางและมาตรการดังต่อไปนี้:

7.1 สิทธิ์ในการติดตามการใช้งานข้อมูล

บริษัทมีสิทธิ์ในการติดตามและเฝ้าระวังการใช้งานข้อมูลในระบบสารสนเทศทั้งหมด รวมถึงแต่ไม่จำกัดเฉพาะ:

- การเข้าถึงข้อมูล
- การโอนย้ายหรือแบ่งปันข้อมูล
- การแก้ไขหรือปรับเปลี่ยนข้อมูล
- การดาวน์โหลดหรือบันทึกข้อมูล

การติดตามจะดำเนินการผ่าน ระบบตรวจสอบอัตโนมัติ เช่น Log Management System, Intrusion Detection System (IDS) และ Data Loss Prevention (DLP)

7.2 การตรวจสอบเชิงรุกและการวิเคราะห์ความเสี่ยง

บริษัทจะดำเนินการ ตรวจสอบเชิงรุก (Proactive Monitoring) เพื่อตรวจจับพฤติกรรมการใช้งานที่ผิดปกติ เช่น:

- การเข้าถึงข้อมูลนอกเวลางาน
- การดาวน์โหลดข้อมูลจำนวนมากในระยะเวลาสั้น
- การพยายามเข้าถึงข้อมูลที่ไม่ได้รับอนุญาต

8. การละเมิดนโยบายและบทลงโทษ (Policy Violations and Penalties)

- พนักงานที่ละเมิดนโยบายการบริหารจัดการข้อมูลสารสนเทศภายในของบริษัทจะต้องรับผิดชอบต่อผลที่เกิดขึ้น และจะถูกลงโทษตามข้อกำหนดขององค์กร รวมถึงการดำเนินคดีตามกฎหมายในกรณีที่เป็นการกระทำที่ผิดกฎหมาย
- บุคคลภายนอกที่ละเมิดนโยบายจะถูกยกเลิกสิทธิ์การเข้าถึงข้อมูลทันทีและอาจถูกดำเนินคดีตามกฎหมาย

PRO INSIDE PUBLIC COMPANY LIMITED
No.55, A.A.Capital Ratchada Building, 5 Floor,
Ratchadapisek Road, Dindaeng, Dindaeng, Bangkok 10400

บริษัท โปร อินไซด์ จำกัด (มหาชน)
เลขที่ 55 อาคารเอ.เอ.แคปปิตอล รัชดา ชั้นที่ 5 ถนนรัชดาภิเษก
แขวงดินแดง เขตดินแดง กรุงเทพมหานคร 10400
เลขประจำตัวผู้เสียภาษี 0107567000023

Tel : +66 2029 7875
Fax: +66 2029 7879

9. การแจ้งเบาะแส

หากผู้ใดพบเห็นการกระทำอันเชื่อได้ว่าเป็นการละเมิดหรือไม่เป็นไปตามนโยบายฉบับนี้ ขอให้ทำการร้องเรียนหรือแจ้งเบาะแสตามขั้นตอนภายใต้นโยบายหรือแนวปฏิบัติเกี่ยวกับการแจ้งเบาะแสทันที ทั้งนี้ผู้ร้องเรียนหรือผู้แจ้งเบาะแสจะได้รับความคุ้มครอง และข้อมูลจะถูกเก็บไว้เป็นความลับ โดยไม่มีผลต่อการปฏิบัติงานทั้งในระหว่างดำเนินการสอบสวนและหลังจากเสร็จสิ้นกระบวนการ

ใหมีผลตั้งแต่วันที่ 1 เมษายน 2568 เป็นตนไป

-วิสุทธิ์ ศรีสุพรรณ-

(นายวิสุทธิ์ ศรีสุพรรณ)

ประธานกรรมการ

อนุมัติโดยที่ประชุมคณะกรรมการบริษัท ครั้งที่ 2/2568

เมื่อวันที่ 24 มีนาคม 2568

PRO INSIDE PUBLIC COMPANY LIMITED
No.55, A.A.Capital Ratchada Building, 5 Floor,
Ratchadapisek Road, Dindaeng, Dindaeng, Bangkok 10400

บริษัท โปร อินไซด์ จำกัด (มหาชน)
เลขที่ 55 อาคารเอ.เอ.แคปปิตอล รัชดา ชั้นที่ 5 ถนนรัชดาภิเษก
แขวงดินแดง เขตดินแดง กรุงเทพมหานคร 10400
เลขประจำตัวผู้เสียภาษี 0107567000023

Tel : +66 2029 7875
Fax: +66 2029 7879