นโยบายการรักษาความปลอดภัยด้านเทคโนโลยีสารสนเทศ
บริษัท สหพัฒนาอินเตอร์โฮลดิ้ง จำกัด (มหาชน)
(ฉบับปรับปรุง ครั้งที่ 2)

บริษัทฯ ให้ความสำคัญกับเทคโนโลยีสารสนเทศและการสื่อสาร ซึ่งเป็นปัจจัยสำคัญในการสนับสนุนและส่งเสริมการดำเนินธุรกิจของบริษัท ดังนั้น เพื่อให้บุคลากรของบริษัทรับทราบถึงหน้าที่ ข้อปฏิบัติเกี่ยวกับระบบเทคโนโลยีสารสนเทศ รวมถึงควบคุมป้องกันปัญหาที่อาจเกิดขึ้นจากการใช้งานระบบเทคโนโลยีสารสนเทศในลักษณะที่ไม่ถูกต้อง และการถูกคุกคามจากภัยต่างๆ ซึ่งเป็นความรับผิดชอบร่วมกันของกรรมการบริษัท ผู้บริหาร พนักงาน และบุคคลที่เกี่ยวข้องทุกคน โดยกำหนดเป็นลายลักษณ์อักษร เพื่อเป็นแนวทางปฏิบัติ ดังนี้

1. ประเมินความเสี่ยงด้านความปลอดภัยของระบบเทคโนโลยีสารสนเทศ และกำหนดขั้นตอนปฏิบัติ เพื่อรับมือกับเหตุการณ์ละเมิดความปลอดภัยที่เกิดขึ้น
2. บริหารทรัพยากรด้านเทคโนโลยีสารสนเทศให้สอดคล้องกับแผนกลยุทธ์ของบริษัท โดยให้ครอบคลุมถึงการบริหารทรัพยากรบุคคล และระบบเทคโนโลยีสารสนเทศที่เพียงพอต่อการดำเนินงานด้านเทคโนโลยีสารสนเทศ
3. ควบคุม ตรวจสอบ การพัฒนา ปรับปรุง แก้ไขเปลี่ยนแปลงระบบเทคโนโลยีสารสนเทศ เพื่อลดความเสี่ยงที่จะทำให้ระบบเทคโนโลยีสารสนเทศเสียหาย ผิดปกติหรือไม่สามารถใช้งานได้ รวมถึงจัดทำวิธีการปฏิบัติในการปรับปรุงเปลี่ยนแปลง แก้ไขระบบเทคโนโลยีสารสนเทศ
4. ตรวจสอบ ควบคุมการเข้าถึงและใช้งานระบบเทคโนโลยีสารสนเทศของผู้บริหาร พนักงาน หรือ ผู้ที่เกี่ยวข้องให้เป็นไปอย่างเหมาะสม และป้องกันการเข้าถึงข้อมูลของผู้ที่ไม่ได้มีอำนาจหน้าที่ หรือ ผู้ที่ไม่ได้รับอนุญาต ที่อาจนำพามาซึ่งความเสี่ยงเกี่ยวกับข้อมูลและการประมวลผลของระบบเทคโนโลยีสารสนเทศ
5. ควบคุมการเข้าออกศูนย์คอมพิวเตอร์และการป้องกันความเสียหายทางกายภาพ จากผู้ที่ไม่มีอำนาจหน้าที่หรือผู้ที่ไม่ได้รับอนุญาต ซึ่งอาจก่อให้เกิดความเสียหายต่อข้อมูลที่จัดเก็บอยู่ในระบบคอมพิวเตอร์
6. สื่อสารข้อตกลงในการใช้งานระบบเทคโนโลยีสารสนเทศให้กับผู้บริหาร พนักงาน และผู้ที่เกี่ยวข้อง เพื่อให้มีการใช้งานที่ถูกต้อง เหมาะสม และเกิดประโยชน์สูงสุด
7. กำหนดให้มีการควบคุมการเข้ารหัสข้อมูล ตามข้อตกลง กฎหมาย และระเบียบที่เกี่ยวข้อง เพื่อให้มีการเข้ารหัสข้อมูลอย่างเหมาะสมและมีประสิทธิภาพ เพื่อป้องกันความลับรั่วไหล การปลอมแปลง หรือ เพื่อความถูกต้องสมบูรณ์ของข้อมูลสารสนเทศในระบบเทคโนโลยีสารสนเทศและการสื่อสารของบริษัท
8. กำหนดรูปแบบการปฏิบัติในการจัดลำดับงานด้านสารสนเทศ การจัดการกับปัญหาของระบบสารสนเทศ เพื่อลดผลกระทบต่อกระบวนการทำงาน สามารถแก้ไขปัญหาให้กลับคืนสู่ภาวะปกติได้เร็วที่สุด การสำรองข้อมูลที่เหมาะสมและการกู้คืนระบบสารสนเทศ เพื่อป้องกันการสูญหายอันเกิดขึ้นจากภาวะฉุกเฉินหรือภัยพิบัติต่างๆ
9. กำหนดให้มีการทบทวนนโยบายการรักษาความปลอดภัยระบบเทคโนโลยีสารสนเทศ อย่างน้อยปีละ 1 ครั้ง หรือ เมื่อมีการเปลี่ยนแปลงที่มีนัยสำคัญ
10. ทุกหน่วยงานมีหน้าที่รับผิดชอบโดยการประกาศให้ทราบ และเผยแพร่นโยบายเหล่านี้ รวมทั้งทำการสนับสนุน ตอบสนอง นโยบายของบริษัท
11. ควบคุมการใช้งานระบบเทคโนโลยีสารสนเทศ ให้เป็นไปตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ และให้เป็นไปตามกฎหมายที่เกี่ยวข้องกับระบบเทคโนโลยีสารสนเทศ

นโยบายการรักษาความปลอดภัยด้านเทคโนโลยีสารสนเทศ (ฉบับปรับปรุง ครั้งที่ 2) นี้ ได้รับอนุมัติโดยมติที่ประชุมคณะกรรมการบริษัท ครั้งที่ 3 (ชุดที่ 31) เมื่อวันที่ 14 สิงหาคม 2567 และมีผลใช้บังคับตั้งแต่วันที่ 15 สิงหาคม 2567 เป็นต้นไป โดยยกเลิกนโยบายการรักษาความปลอดภัยด้านเทคโนโลยีสารสนเทศ (ฉบับปรับปรุง ครั้งที่ 1) ที่มีผลใช้บังคับเมื่อวันที่ 17 ธันวาคม 2564 ที่ได้รับอนุมัติจากที่ประชุมคณะกรรมการบริษัทครั้งที่ 9 (ชุดที่ 28) เมื่อวันที่ 16 ธันวาคม 2564

(นายสมคิด จาตุศรีพิทักษ์)
ประธานกรรมการบริษัท