



นโยบายการรักษาความปลอดภัยด้านเทคโนโลยีสารสนเทศ
บริษัท สหพัฒนานินเตอร์โฮลดิ้ง จำกัด (มหาชน)
(ฉบับปรับปรุง ครั้งที่ 3)

บริษัทฯ ให้ความสำคัญกับเทคโนโลยีสารสนเทศและการสื่อสาร ซึ่งเป็นปัจจัยสำคัญในการสนับสนุนและส่งเสริมการดำเนินธุรกิจของบริษัท ดังนั้น เพื่อให้บุคลากรของบริษัททราบถึงหน้าที่ ข้อปฏิบัติเกี่ยวกับระบบเทคโนโลยีสารสนเทศ รวมถึงควบคุมป้องกันปัญหาที่อาจเกิดขึ้นจากการใช้งานระบบเทคโนโลยีสารสนเทศในลักษณะที่ไม่ถูกต้อง และการถูกคุกคามจากภัยต่างๆ ซึ่งเป็นความรับผิดชอบร่วมกันของกรรมการบริษัท ผู้บริหาร พนักงานบริษัท และบุคคลที่เกี่ยวข้องทุกคน โดยกำหนดเป็นลายลักษณ์อักษร เพื่อเป็นแนวทางปฏิบัติ ดังนี้

1. ประเมินความเสี่ยงด้านความปลอดภัยของระบบเทคโนโลยีสารสนเทศและกำหนดขั้นตอนปฏิบัติ เพื่อรับมือกับเหตุการณ์ละเมิดความปลอดภัยที่เกิดขึ้น
2. บริหารทรัพยากรด้านเทคโนโลยีสารสนเทศให้สอดคล้องกับแผนกลยุทธ์บริษัทฯ โดยให้ครอบคลุมถึงการบริหารทรัพยากรบุคคลและระบบเทคโนโลยีสารสนเทศที่เพียงพอต่อการดำเนินงานด้านเทคโนโลยีสารสนเทศ
3. ควบคุม ตรวจสอบ การพัฒนา ปรับปรุง แก้ไขเปลี่ยนแปลงระบบเทคโนโลยีสารสนเทศ เพื่อลดความเสี่ยงที่จะทำให้ระบบเทคโนโลยีสารสนเทศเสียหาย ผิดพลาดหรือไม่สามารถใช้งานได้ รวมถึงจัดทำวิธีการปฏิบัติในการปรับปรุงเปลี่ยนแปลง แก่ระบบเทคโนโลยีสารสนเทศ
4. ตรวจสอบ ควบคุมการเข้าถึงและใช้งานระบบเทคโนโลยีสารสนเทศของผู้บริหาร พนักงาน หรือ ผู้ที่เกี่ยวข้องให้เป็นไปอย่างเหมาะสม และป้องกันการเข้าถึงข้อมูลของผู้ที่ไม่ได้อ่านาหน้าหรือ ผู้ที่ไม่ได้รับอนุญาต ที่อาจนำมาซึ่งความเสี่ยงเกี่ยวกับข้อมูลและการประมวลผลของระบบเทคโนโลยีสารสนเทศ
5. ควบคุมการเข้าออกศูนย์คอมพิวเตอร์และการป้องกันความเสียหายทางกายภาพ จากผู้ที่ไม่ได้อ่านาหน้าหรือผู้ที่ไม่ได้รับอนุญาต ซึ่งอาจก่อให้เกิดความเสียหายต่อข้อมูลที่จัดเก็บอยู่ในระบบคอมพิวเตอร์
6. สื่อสารข้อตกลงในการใช้งานระบบเทคโนโลยีสารสนเทศให้กับผู้บริหาร พนักงานและผู้ที่เกี่ยวข้อง เพื่อให้มีการใช้งานที่ถูกต้อง เหมาะสม และเกิดประโยชน์สูงสุด
7. กำหนดให้มีการควบคุมการเข้ารหัสข้อมูล ตามข้อตกลง กฎหมาย และระเบียบที่เกี่ยวข้อง เพื่อให้มีการเข้ารหัสข้อมูลอย่างเหมาะสมและได้ผล และเพื่อป้องกันการความลับ การปลอมแปลง หรือความถูกต้องสมบูรณ์ของข้อมูลของสารสนเทศในระบบเทคโนโลยีสารสนเทศและการสื่อสารของบริษัท
8. กำหนดรูปแบบการปฏิบัติในการจัดลำดับงานด้านสารสนเทศ การจัดการกับปัญหาของระบบสารสนเทศ เพื่อลดผลกระทบต่อกระบวนการทำงาน สามารถแก้ไขปัญหาก็กลับคืนสู่ภาวะปกติได้เร็วที่สุด การสำรองข้อมูลที่เหมาะสมและการกู้คืนระบบสารสนเทศ เพื่อป้องกันการสูญหายอันเกิดขึ้นจากภาวะฉุกเฉินหรือภัยพิบัติต่างๆ
9. กำหนดให้มีการทบทวนนโยบายการรักษาความปลอดภัยระบบเทคโนโลยีสารสนเทศ อย่างน้อยปีละ 1 ครั้ง หรือ เมื่อมีการเปลี่ยนแปลงที่มีนัยสำคัญ
10. ทุกหน่วยงานมีหน้าที่รับผิดชอบโดยการประกาศให้ทราบ และเผยแพร่ นโยบายเหล่านี้ รวมทั้งทำการสนับสนุน ตอบสนอง นโยบายของบริษัท
11. ควบคุมการใช้งานระบบเทคโนโลยีสารสนเทศ ให้เป็นไปตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ และให้เป็นไปตามกฎหมายที่เกี่ยวข้องกับระบบเทคโนโลยีสารสนเทศ
12. กำหนดให้มีการใช้งานปัญญาประดิษฐ์ (AI) อย่างมีจริยธรรม ปลอดภัย โปร่งใส และอยู่ภายใต้การควบคุมที่เหมาะสม โดยต้องไม่ละเมิดสิทธิส่วนบุคคลหรือก่อให้เกิดความเสี่ยงต่อข้อมูลและระบบสารสนเทศของบริษัท

นโยบายการรักษาความปลอดภัยด้านเทคโนโลยีสารสนเทศ (ฉบับปรับปรุง ครั้งที่ 3) นี้ ได้รับอนุมัติโดยมติที่ประชุมคณะกรรมการบริษัท ครั้งที่ 5 (ชุดที่ 32) เมื่อวันที่ 18 กันยายน 2568 และมีผลใช้บังคับตั้งแต่วันที่ 19 กันยายน 2568 เป็นต้นไป โดยยกเลิกนโยบายการรักษาความปลอดภัยด้านเทคโนโลยีสารสนเทศ (ฉบับปรับปรุง ครั้งที่ 2) ที่มีผลใช้บังคับเมื่อวันที่ 15 สิงหาคม 2567 ที่ได้รับอนุมัติจากที่ประชุมคณะกรรมการบริษัท ครั้งที่ 3 (ชุดที่ 31) เมื่อวันที่ 14 สิงหาคม 2567

นายสมคิด จาตุศรีพิทักษ์
ประธานกรรมการบริษัท