ANANDA

นโยบายด้านเทคโนโลยีและสารสนเทศ

บริษัท อนันดา ดีเวลลอปเม้นท์ จำกัด (มหาชน) และบริษัทในเครือ

อนุมัติโดยที่ประชุมคณะกรรมการบริษัท ครั้งที่ 1/2568 เมื่อวันที่ 27 กุมภาพันธ์ 2568

1. **หลักการและเหตุผล**

บริษัท อนันดา ดีเวลลอปเม้นท์ จำกัด (มหาชน) ตระหนักถึงความสำคัญของการนำเทคโนโลยีสารสนเทศมาใช้ในการบริหารจัดการธุรกิจ จึงกำหนดนโยบายฉบับนี้เพื่อให้บริษัทมีกรอบการกำกับดูแลและบริหารจัดการเทคโนโลยีสารสนเทศในระดับองค์กรที่ดี โดยอ้างอิงแนวปฏิบัติ ตาม มาตรฐาน ISO 27001-มาปรับใช้ให้เหมาะสมกับบริบทการดำเนินธุรกิจของบริษัท รวมถึงเพื่อให้บริษัทสามารถดำเนินกิจการให้บรรลุวัตถุประสงค์และเป้าหมาย โดยมีการใช้ทรัพยากรและการบริหารจัดการความเสี่ยงอย่างเหมาะสม สอดคล้องกับการกำกับดูแลกิจการที่ดี

2. **วัตถุประสงค์**

เพื่อให้บริษัท มีกรอบการกำกับดูแลและการบริหารจัดการเทคโนโลยีสารสนเทศระดับองค์กรที่ดีที่สอดคล้องกับมาตรฐาน ISO 27001 และการดำเนินธุรกิจของบริษัท บริษัทจึงได้กำหนดนโยบายฯ ฉบับนี้ขึ้น โดยมีวัตถุประสงค์ดังต่อไปนี้

1. เพื่อให้มีนโยบายการบริหารจัดการเทคโนโลยีสารสนเทศ อย่างมีประสิทธิภาพ และประสิทธิผล ให้เกิดประโยชน์สูงสุดในการดำเนินกิจการของบริษัทให้เจริญเติบโตอย่างยั่งยืน และมีมาตรฐาน
2. เพื่อให้เป็นกรอบแนวทางในการกำหนดระเบียบปฏิบัติงานหรือคู่มือปฏิบัติงานที่เกี่ยวข้องได้แก่ ระเบียบปฏิบัติงานในด้านการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ ระเบียบปฏิบัติงานบริหารความเสี่ยงของระบบเทคโนโลยีสารสนเทศและคู่มือปฏิบัติงานในเรื่องต่างๆ
3. เพื่อรักษาความมั่นคงปลอดภัยสารสนเทศให้มีการบริหารความเสี่ยง การปกป้องดูแล การติดตาม การเฝ้าระวัง การตรวจสอบและการควบคุมให้เป็นไปตามกฎหมาย กฎระเบียบ และมาตรฐานที่เกี่ยวข้องโดยยึดหลักการรักษาความลับ (Confidentiality) ความถูกต้องครบถ้วน (Integrity) ความพร้อมใช้งานของสินทรัพย์สารสนเทศ (Availability) และความปลอดภัย(Safety) เพื่อสร้างความต่อเนื่องในการทำธุรกิจ สร้างวัฒนธรรมด้านความปลอดภัยที่เข้มแข็งและเพิ่มขีดความสามารถทางการแข่งขันอย่างยั่งยืน

3. **ขอบเขตของนโยบาย**

นโยบายฯ ฉบับนี้มีผลบังคับใช้กับบริษัท ซึ่งครอบคลุมถึงข้อมูลหรือสารสนเทศ (Data/Information) ระบบปฏิบัติการ (Operating System) ระบบงาน (Application System) ระบบฐานข้อมูล (Database System) อุปกรณ์คอมพิวเตอร์ (Hardware) และระบบเครือข่ายสื่อสาร (Network/Communication System) ภายใต้นโยบายฉบับนี้ บริษัทต้องจัดให้มีหลักเกณฑ์ด้านเทคโนโลยีสารสนเทศดังนี้

3.1 โครงสร้างการบริหารงานเพื่อการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ (organization of information technology security) โดยกำหนดหน้าที่และความรับผิดชอบของบุคลากร รวมถึงการสอบทานการปฏิบัติงานเพื่อป้องกันความเสี่ยงในการรักษาความมั่นคงปลอดภัยของระบบ เทคโนโลยีสารสนเทศ ที่อาจเกิดขึ้นในการปฏิบัติงาน โดยมีการควบคุมเหตุการณ์ที่เกี่ยวข้องกับความเสี่ยงในระบบหลัก รวมทั้งความเสี่ยงที่เกี่ยวข้องกับการสำรองข้อมูลผิดพลาดและการติดตามตรวจสอบรวมทั้งการสอบทานผลกระทบจากการใช้งานในระบบหลัก เพื่อนำมาแก้ไขระบบรวมทั้งการป้องกันมิให้เกิดความผิดพลาดที่เกิดขึ้น

3.2 การบริหารจัดการกับบุคลากร และผู้ให้บริการภายนอก ที่เกี่ยวข้องหรือที่ใช้ระบบเทคโนโลยีสารสนเทศปฏิบัติงาน และผู้ให้บริการภายนอก ในกรณีที่บริษัทมีการดำเนินการใช้บริการงานด้าน เทคโนโลยีสารสนเทศจากผู้ให้บริการภายนอก เชื่อมต่อระบบ เทคโนโลยีสารสนเทศ กับผู้ให้บริการภายนอก อนุญาตให้ผู้ให้บริการภายนอก สามารถเข้าถึงข้อมูลสำคัญหรือข้อมูลของลูกค้าที่ควบคุมดูแลโดยบริษัทได้ โดยต้องกำหนดให้มี

มาตรการในการกำกับดูแลและควบคุมรวมทั้งการบริหารจัดการไม่ให้เกิดการละเมิดสิทธิ์การเข้าถึงและการปรับปรุงแก้ไขต่างๆที่ไม่ได้รับการอนุญาต

3.3 การบริหารจัดการทรัพย์สินด้านเทคโนโลยีสารสนเทศ (IT asset management) เพื่อนำไปใช้ดำเนินการเกี่ยวกับการรักษาความมั่นคงปลอดภัยด้าน เทคโนโลยีสารสนเทศ ได้อย่างเหมาะสม ครบถ้วนและเป็นปัจจุบัน โดยที่ทรัพย์สินด้านเทคโนโลยีสารสนเทศต้องได้รับการปกป้องและควบคุมความเสียหายหรือผลกระทบจากภัยด้านเทคโนโลยีสารสนเทศในรูปแบบต่างๆ จากภายนอกองค์กร

3.4 การรักษาความมั่นคงปลอดภัยของข้อมูล (data security) เพื่อให้ข้อมูลมีความถูกต้องครบถ้วน และมีสภาพพร้อมใช้งาน โดยต้องกำหนดให้มีมาตรการในการรักษาความลับของข้อมูลและใช้งานได้อย่างเหมาะสม

3.5 การควบคุมการเข้าถึงข้อมูลและระบบเทคโนโลยีสารสนเทศ (access control) อย่างมีประสิทธิภาพ เพื่อให้สามารถ ป้องกันการเข้าถึง โดยต้องกำหนดมาตรการในการกำกับดูแลและควบคุมรวมทั้งป้องกันมิให้เกิดผลกระทบจากการเปลี่ยนแปลงแก้ไขโดยผู้ไม่มีสิทธิหรือไม่ได้รับอนุญาต

3.6 การควบคุมการเข้ารหัส (cryptographic control) ที่เชื่อถือได้และมีความปลอดภัยเป็นไปตามมาตรฐานสากล เพื่อให้มั่นใจได้ว่า การธำรงไว้ซึ่งความลับ (Confidentiality) ความถูกต้องครบถ้วน (Integrity) และความถูกต้องแท้จริง (Authenticity) ของข้อมูล โดยจัดหาวิธีการและช่องทางที่มีความเหมาะสม มีประสิทธิภาพ

3.7 การรักษาความมั่นคงปลอดภัยทางกายภาพและสภาพแวดล้อม (physical and environmental security) ของทรัพย์สิน ด้านเทคโนโลยีสารสนเทศ เพื่อให้สามารถป้องกันความเสียหายต่อทรัพย์สินด้านเทคโนโลยีสารสนเทศที่จัดเก็บอยู่ในศูนย์คอมพิวเตอร์หลัก ศูนย์คอมพิวเตอร์สำรอง และศูนย์คอมพิวเตอร์จากบุคคลภายนอก (Co-location) โดยต้องกำหนดเงื่อนไขในการเข้าถึงอุปกรณ์และพื้นที่สำคัญที่เกี่ยวกับความมั่นคงและปลอดภัยในระบบเทคโนโลยีสารสนเทศ

3.8 การรักษาความมั่นคงปลอดภัยในการปฏิบัติงานด้าน เทคโนโลยีสารสนเทศ (IT operation security) เพื่อให้การปฏิบัติงานเกี่ยวกับการประมวลผลข้อมูลมีความถูกต้องและมั่นคงปลอดภัย ซึ่งครอบคลุมการบริหารจัดการในเรื่อง การตั้งค่าระบบ (System Configuration Management) การเปลี่ยนแปลง (Change Management) ขีดความสามารถของระบบ เทคโนโลยีสารสนเทศ (Capacity Management) การรักษาความมั่นคงปลอดภัยของเครื่องแม่ข่าย (Server) และอุปกรณ์ที่ใช้ปฏิบัติงาน (Endpoint) การใช้งานอุปกรณ์เคลื่อนที่ (mobile device) และรวมถึงการใช้งานอุปกรณ์ส่วนตัว (Bring Your Own Device: BYOD) การสำรองข้อมูล (data backup) การจัดเก็บข้อมูลบันทึกเหตุการณ์การใช้งานเกี่ยวกับระบบ IT (Log) การติดตามดูแลระบบและเฝ้าระวังภัยคุกคามทางไซเบอร์ (cyber security) โดยต้องมีการกำหนดมาตรการในการกำกับดูแลควบคุมรวมทั้งบริหารจัดการปัจจัยที่อาจทำให้เกิดผลกระทบด้านความเสียหายจากระบบการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศอันส่งผลกระทบต่อระบบการรักษาความมั่นคงปลอดภัยในการปฏิบัติงานด้าน เทคโนโลยีสารสนเทศ

3.9 การรักษาความมั่นคงปลอดภัยเกี่ยวกับระบบเครือข่ายสื่อสาร (network security) อย่างเหมาะสม เพื่อให้ระบบเครือข่ายสื่อสารและข้อมูลที่รับส่งผ่านระบบเครือข่ายสื่อสารมีความมั่นคงปลอดภัย ให้บริการได้อย่างมีประสิทธิภาพ โดยต้องกำหนดให้มีมาตรการในการกำกับดูแลและควบคุมรวมทั้งการบริหารจัดการความเสี่ยงที่เกิดจากระบบเครือข่ายสื่อสาร

3.10 การบริหารจัดการโครงการด้าน เทคโนโลยีสารสนเทศ (IT project management) เพื่อให้มั่นใจว่ามีการรักษาความมั่นคงปลอดภัยตลอดวงจรชีวิตของระบบ เทคโนโลยีสารสนเทศ (entire life cycle) โดยต้องกำหนดให้มีมาตรการในการบริหาร จัดหา และเปลี่ยนแปลง รวมทั้งมีการพัฒนาอย่างต่อเนื่องและเหมาะสม

3.11การบริหารจัดการเหตุการณ์ผิดปกติด้าน เทคโนโลยีสารสนเทศ (IT incident management) เพื่อให้การปฏิบัติงานด้านเทคโนโลยีสารสนเทศกลับมาทำงานได้อย่างมีประสิทธิภาพเหมือนเดิมโดยเร็วที่สุด โดยต้องมีมาตรการในการบริหารจัดการเหตุการณ์ผิดปกติ อย่างเป็นกระบวนการ มีขั้นตอนที่เหมาะสมและทันท่วงที

3.12แผนฉุกเฉินด้าน เทคโนโลยีสารสนเทศ (IT disaster recovery plan) เพื่อรองรับเหตุการณ์ผิดปกติด้านเทคโนโลยีสารสนเทศ ซึ่งส่งผลกระทบ ให้ไม่สามารถให้บริการได้ตามปกติ หรือไม่สามารถดำเนินธุรกิจอย่างต่อเนื่องภายในระยะเวลาที่เหมาะสมได้ โดยต้องจัดทำแผนฉุกเฉินในการกู้คืนระบบให้กลับคืนสู่สภาพปกติภายในระยะเวลาที่เหมาะสม และมีการทดสอบแผนอย่างสม่ำเสมอ

4. <u>คำจำกัดความ</u>

- **บริษัท** หมายถึง บริษัท อนันดา ดีเวลลอปเม้นท์ จำกัด (มหาชน) และบริษัทย่อย

- **นโยบายฯ** หมายถึง นโยบายด้านเทคโนโลยีสารสนเทศ

- **ผู้ใช้งานระบบเทคโนโลยีสารสนเทศ** หมายถึง พนักงานประจำ พนักงานตามสัญญาจ้าง ผู้ให้บริการภายนอก ผู้ใช้งานภายนอก คู่ค้า หรือลูกค้าของบริษัท

- **ผู้ให้บริการภายนอก** หมายถึง บุคคลหรือนิติบุคคลจากภายนอกองค์กร ซึ่งบริษัทว่าจ้างเพื่อใช้บริการที่เกี่ยวข้องกับระบบสารสนเทศ

- **ผู้ใช้งานภายนอก** หมายถึง บุคคลหรือนิติบุคคลจากภายนอกองค์กร ที่มีความจำเป็นต้องใช้งานระบบเทคโนโลยีสารสนเทศ ในเนื้อหาไม่มีคำนี้? หรือพี่หาไม่เจอ มีแต่บุคคลากรภายนอก

- **ระบบเทคโนโลยีสารสนเทศ** หมายถึง ระบบคอมพิวเตอร์ที่หน่วยงานเทคโนโลยีสารสนเทศให้บริการ

- **ระบบเครือข่ายคอมพิวเตอร์** หมายถึง ระบบที่สามารถใช้ในการติดต่อสื่อสาร หรือการส่งข้อมูล และสารสนเทศระหว่างระบบเทคโนโลยีสารสนเทศได้

- **ระบบคอมพิวเตอร์** หมายถึง อุปกรณ์ หรือชุดอุปกรณ์ของคอมพิวเตอร์ที่เชื่อมการทำงานเข้าด้วยกันโดยได้มีการกำหนดคำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใด และแนวทางปฏิบัติงานให้อุปกรณ์ หรือชุดอุปกรณ์ทำหน้าที่ประมวลผลข้อมูลโดยอัตโนมัติ

- **ระบบสารสนเทศ** หมายถึง ระบบงานที่ใช้จัดเก็บและประมวลผลข้อมูลซึ่งทำงานประสานกันระหว่างฮาร์ดแวร์ ซอฟต์แวร์ ข้อมูล ผู้ใช้งาน และกระบวนการประมวลผลให้เกิดเป็นข้อมูลสารสนเทศที่สามารถนำไปใช้ประโยชน์ในการวางแผน การบริหาร การสนับสนุนการให้บริการ

- **ทรัพย์สินสารสนเทศ** หมายถึง

1) ทรัพย์สินสารสนเทศประเภทระบบ ได้แก่ ระบบเครือข่ายคอมพิวเตอร์ ระบบคอมพิวเตอร์ ระบบงานคอมพิวเตอร์ ระบบเทคโนโลยีสารสนเทศ

2) ทรัพย์สินสารสนเทศประเภทอุปกรณ์ ได้แก่ ตัวเครื่องคอมพิวเตอร์ อุปกรณ์คอมพิวเตอร์ เครื่องบันทึกข้อมูล อุปกรณ์เครือข่าย และอุปกรณ์อื่นใด

3) ทรัพย์สินสารสนเทศประเภทข้อมูล ได้แก่ ข้อมูลสารสนเทศ ข้อมูลอิเล็กทรอนิกส์ และข้อมูลคอมพิวเตอร์

4) ทรัพย์สินสารสนเทศประเภทลิขสิทธิ์ คือ ทรัพย์สินที่เกิดการพัฒนา หรือสิทธิ์ในการใช้จากเจ้าของผลิตภัณฑ์

- **หน่วยงานเทคโนโลยีสารสนเทศ** หมายถึง หน่วยงานตามโครงสร้างของบริษัทที่มีหน้าที่รับผิดชอบงานด้านเทคโนโลยีสารสนเทศ

5. บทบาทและความรับผิดชอบในการปฏิบัติตามนโยบายฉบับนี้

5.1 คณะกรรมการบริษัท

5.1.1 กำกับดูแลให้คณะกรรมการบริหารปฏิบัติตามนโยบายฯ ให้สอดคล้องกับความต้องการของบริษัท รวมทั้งสนับสนุนและพัฒนาการดำเนินธุรกิจ การบริหารความเสี่ยง เพื่อให้สามารถบรรลุวัตถุประสงค์และเป้าหมายหลักของบริษัท

5.2 คณะกรรมการบริหาร

5.2.1 กำหนดแนวปฏิบัติ หลักเกณฑ์ และระเบียบปฏิบัติที่เกี่ยวข้องกับนโยบายฯ

5.2.2 ติดตามควบคุมและกำกับดูแลให้หน่วยงานที่เกี่ยวข้องดำเนินการตามนโยบายฯ ที่กำหนด

5.3 หน่วยงานเทคโนโลยีสารสนเทศ

5.3.1 ติดตามดูแลให้ผู้ใช้งานปฏิบัติตามนโยบายฯ หลักเกณฑ์ระเบียบปฏิบัติที่เกี่ยวข้องอย่างถูกต้องเหมาะสม และหากมีการปฏิบัติที่ไม่ถูกต้องให้รายงานต่อคณะกรรมการบริหารทราบ

5.3.2 สื่อสารนโยบายฯ ให้แก่ผู้ใช้งาน ในลักษณะที่สามารถเข้าถึงได้ง่าย เพื่อให้บุคลากรดังกล่าวเข้าใจ และสามารถปฏิบัติตามนโยบายดังกล่าวได้อย่างถูกต้อง

5.3.3 ทบทวนหรือปรับปรุงนโยบายฯ อย่างน้อยปีละ 1ครั้ง หรือเมื่อมีเหตุการณ์ใด ๆ ซึ่งอาจส่งผลกระทบต่อการกำกับดูแลและบริหารจัดการเทคโนโลยีสารสนเทศอย่างมีนัยสำคัญ

5.4 ผู้ใช้งานระบบเทคโนโลยีสารสนเทศ

5.4.1 เรียนรู้ ทำความเข้าใจ และปฏิบัติตามนโยบายฯ มาตรฐานการปฏิบัติงาน และกระบวนการปฏิบัติงาน ได้อย่างถูกต้อง

5.4.2 แจ้งเบาะแสเมื่อพบกรณีกระทำผิดหรือการกระทำที่อาจเข้าข่ายฝ่าฝืนนโยบายฯ

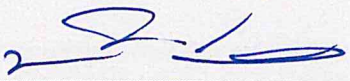
6. การติดตามการปฏิบัติตามนโยบาย

กำหนดให้ต้องมีการติดตามและประเมินผลการปฏิบัติตามนโยบายอย่างน้อยปีละ 1 ครั้งโดยใช้เอกสารรายละเอียดระเบียบปฏิบัติงานในด้านการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ

7. การทบทวนนโยบาย

กำหนดให้หน่วยงานเทคโนโลยีสารสนเทศมีการทบทวนนโยบายฯ ให้เป็นปัจจุบันอย่างน้อยปีละ 1 ครั้ง หรือเมื่อมีเหตุการณ์ใด ๆ ซึ่งอาจส่งผลกระทบต่อการกำกับดูแลและบริหารจัดการเทคโนโลยีสารสนเทศอย่างมีนัยสำคัญ

นโยบายฯ ฉบับนี้ได้รับอนุมัติจากคณะกรรมการบริษัทในการประชุมครั้งที่ xx/256x เมื่อวันที่ XX เดือน 256x เป็นต้นไป



(ดร.ณรงค์ชัย อัครเศรณี)

ประธานกรรมการ
บริษัท อนันดา ดีเวลลอปเม้นท์ จำกัด (มหาชน)