นโยบายด้านความมั่นคงปลอดภัยสารสนเทศ
บริษัท น้ำมันพืชไทย จำกัด (มหาชน)

1 หลักการ / INTRODUCTION

เทคโนโลยีสารสนเทศได้เข้ามามีบทบาทสำคัญในการดำเนินธุรกิจของบริษัท น้ำมันพืชไทย จำกัด (มหาชน) (บริษัท) ทั้งในเรื่องของการบริหารจัดการ การจัดเก็บข้อมูล และการประมวลผลข้อมูล ทำให้การดำเนินงานมีความสะดวก รวดเร็ว มีประสิทธิภาพ และเพิ่มโอกาสในการแข่งขันทางธุรกิจได้มากขึ้น

อย่างไรก็ตาม การนำเทคโนโลยีเข้ามาใช้อาจนำมาซึ่งความเสี่ยงจากภัยคุกคามหลายรูปแบบ ซึ่งหากไม่มีการบริหารจัดการความมั่นคงปลอดภัยด้านสารสนเทศที่เหมาะสมและรัดกุมเพียงพอ อาจทำให้สารสนเทศเหล่านั้นถูกเปิดเผย แก้ไขเปลี่ยนแปลง ทำลาย หรือสูญหาย และอาจส่งผลกระทบต่อการดำเนินธุรกิจ ภาพลักษณ์ และชื่อเสียงของบริษัทได้

ผู้บริหารสูงสุดของบริษัท จึงกำหนดนโยบายความมั่นคงปลอดภัยด้านสารสนเทศขึ้น เพื่อใช้เป็นหลักในการบริหารจัดการความมั่นคงปลอดภัยด้านสารสนเทศให้สอดคล้องกับการดำเนินงานและวัตถุประสงค์ในการดำเนินธุรกิจ และได้จัดทำมาตรฐานการปฏิบัติงานด้านความมั่นคงปลอดภัยสารสนเทศ พร้อมกำหนดให้พนักงานของกลุ่มบริษัททุกคนต้องปฏิบัติตามอย่างเคร่งครัด

2 ขอบเขต / SCOPE OF POLICY

มาตรฐานการปฏิบัติงานด้านความมั่นคงปลอดภัยสารสนเทศ ครอบคลุมการป้องกันและการรักษาความมั่นคงปลอดภัยของสารสนเทศของบริษัท ทั้งที่อยู่ภายในสถานที่ปฏิบัติงานของหน่วยงานภายใน และของหน่วยงานภายนอกที่เกี่ยวข้อง โดยครอบคลุมถึง

1. พนักงานและหน่วยงานทั้งหมดของบริษัท
2. พนักงานและหน่วยงานภายนอกที่ได้รับสิทธิในการเข้าถึงทรัพย์สินที่เกี่ยวข้องกับสารสนเทศของบริษัท

3 นิยาม

ความมั่นคงปลอดภัยด้านสารสนเทศ : การป้องกันสารสนเทศจากภัยคุกคามต่าง ๆ เพื่อทำให้มั่นใจว่าการดำเนินธุรกิจจะมีความต่อเนื่อง ลดความเสี่ยงทางธุรกิจ รวมถึงเพิ่มผลตอบแทนการลงทุนและโอกาสในการดำเนินธุรกิจของกลุ่มบริษัท

บริษัท : บริษัท น้ำมันพืชไทย จำกัด (มหาชน)

การแจ้งเตือน (การแจ้งเตือนที่เกี่ยวกับความมั่นคงปลอดภัยด้านสารสนเทศ) : การแจ้งเตือนเกี่ยวกับความมั่นคงปลอดภัยด้านสารสนเทศจากแหล่งต่าง ๆ ซึ่งรวมถึง บุคลากร ระบบ และข้อมูลที่เปิดเผยต่อสาธารณะ

การโจมตี : ความพยายามที่ได้รับอนุญาต หรือไม่ได้รับอนุญาต ไม่ว่าจะสำเร็จหรือไม่ ในการทำลาย แก้ไข ปิดการใช้งาน เข้าถึงสินทรัพย์ หรือพยายามเปิดเผย ขโมย หรือใช้สินทรัพย์โดยไม่ได้รับอนุญาต

จุดอ่อน หรือช่องโหว่ : เป็นสาเหตุ หรือข้อบกพร่องที่เป็นช่องทางที่ก่อให้เกิดภัยคุกคาม

ทีมตอบสนองต่อเหตุการณ์ละเมิดความมั่นคงปลอดภัยด้านสารสนเทศ : ทีมที่ได้รับการแต่งตั้งโดยผู้บริหารสูงสุด ซึ่งประกอบด้วยบุคลากรที่มีทักษะและประสบการณ์ที่เพียงพอ และได้รับการจัดสรรทรัพยากรและอุปกรณ์อำนวยความสะดวกในการทำงานอย่างเหมาะสม ทำหน้าที่จัดการงานที่เกี่ยวข้องกับความมั่นคงปลอดภัยด้านสารสนเทศ ไม่ว่าจะเป็นเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัยด้านสารสนเทศ เหตุการณ์ละเมิดความมั่นคงปลอดภัยด้านสารสนเทศ หรือช่องโหว่

เทคโนโลยีเชิงปฏิบัติการ : Industrial Control Systems (ICS), Supervisory Control and Data Acquisition (SCADA) Systems, Distributed Control Systems (DCS), Programmable Logic Controllers (PLCs), Internet of Things (IoT), Robotics and Automation System และระบบอื่น ๆ ที่ทำงานเกี่ยวกับ Industrial Control

เป้าหมายด้านข้อมูลของการกู้คืนสภาพ (Recovery Point Objective: RPO) : จุดของข้อมูลล่าสุดที่ต้องสามารถนำกลับคืนมาได้เมื่อเกิดความเสียหายต่อระบบสารสนเทศ

เป้าหมายด้านระยะเวลาที่ใช้ในการกู้คืนสภาพ (Recovery Time Objective: RTO) : ระยะเวลาสูงสุดที่ยอมรับได้ในการกู้คืนสภาพจากการหยุดชะงักของการปฏิบัติงานทางธุรกิจ การให้บริการ หรือระบบสารสนเทศ ให้กลับมาให้บริการได้ดังปกติจากจุดที่เกิดความเสียหาย หรือการหยุดชะงักอันเนื่องมาจากเหตุฉุกเฉินหรือภัยพิบัติ

โปรแกรมที่ไม่ประสงค์ดี : โปรแกรม หรือชุดโปรแกรมที่ทำให้สารสนเทศ หรือระบบสารสนเทศเกิดความเสียหายโดยตั้งใจ เช่น ไวรัส (Virus) เวิร์ม (Worm) โทรจัน (Trojan) แอดแวร์ (Adware) หรือสปายแวร์ (Spyware) เป็นต้น

ภัยคุกคาม : เหตุการณ์ หรือสิ่งที่เกิดขึ้นจากภายใน หรือภายนอก และส่งผลเสียต่อทรัพย์สินของบริษัท

เหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัยด้านสารสนเทศ : เหตุการณ์ที่เกิดกับระบบ บริการ (Services) หรือเครือข่าย ที่บ่งชี้ว่าอาจมีการละเมิดนโยบายการปฏิบัติงานด้านความมั่นคงปลอดภัยสารสนเทศ หรือการล้มเหลวของการควบคุม หรือสถานการณ์ที่ไม่ทราบมาก่อนที่อาจเกี่ยวข้องกับความมั่นคงปลอดภัย ทั้งนี้ เหตุการณ์อาจมี หรือไม่มีผลกระทบต่อบริษัท

เหตุการณ์ละเมิดความมั่นคงปลอดภัยด้านสารสนเทศ : เหตุการณ์เดียว หรือหลายเหตุการณ์ที่เกิดขึ้นอย่างต่อเนื่องโดยไม่เป็นที่ต้องการและไม่ได้คาดการณ์ไว้ ที่มีความเป็นไปได้ที่จะส่งผลกระทบต่อการดำเนินธุรกิจและเป็นอันตรายต่อความมั่นคงปลอดภัยด้านสารสนเทศ อีกนัยหนึ่ง เหตุการณ์ที่มีความ

เป็นไปได้ที่จะส่งผลกระทบต่อกลุ่มบริษัท จะถูกพิจารณาเพื่อยืนยันว่าเป็นเหตุการณ์ละเมิดความมั่นคงปลอดภัยด้านสารสนเทศ

หน่วยงานภายนอก: หน่วยงาน หรือบุคคลภายนอกที่ดำเนินธุรกิจ หรือให้บริการ และอาจได้รับสิทธิในการเข้าถึงทรัพย์สินของกลุ่มบริษัท โดยหน่วยงานภายนอกครอบคลุมถึง

1. ผู้รับจ้างปฏิบัติงานให้กับบริษัท (Outsourcer) เช่น ผู้รับจ้างผลิตส่วนประกอบสินค้า ผู้รับจ้างผลิตโฆษณา ผู้รับจ้างผลิตบรรจุภัณฑ์ เป็นต้น
2. ผู้พัฒนาระบบงาน หรือผู้จัดหาวัสดุอุปกรณ์ต่าง ๆ (Supplier) เช่น ผู้พัฒนาระบบงานควบคุมการผลิต ผู้จำหน่ายอุปกรณ์คอมพิวเตอร์ เป็นต้น
3. ผู้ให้บริการต่าง ๆ (Service Provider) เช่น ผู้ติดตั้งและบำรุงรักษาทรัพย์สินต่าง ๆ ผู้ให้บริการโครงข่ายสื่อสาร ผู้ให้บริการอินเทอร์เน็ต เป็นต้น
4. ที่ปรึกษา (Consultant) เช่น ที่ปรึกษาระบบงาน ERP เป็นต้น
5. บริษัทคู่ค้า (Partner)
6. หน่วยงานภายนอกอื่นใด ที่ได้รับสิทธิในการเข้าถึงทรัพย์สิน หรือข้อมูลสารสนเทศขององค์กร

4 นโยบายความมั่นคงปลอดภัยด้านสารสนเทศ

นโยบายความมั่นคงปลอดภัยด้านสารสนเทศ ตามมาตรฐาน ISO/IEC 27001:2022 เป็นกรอบการทำงานที่ครอบคลุมสำหรับการจัดการความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศในทุกมิติ ตั้งแต่มาตรการกำกับดูแลขององค์กร (Organizational Controls) มาตรการด้านบุคลากร (People Controls) มาตรการรักษาความปลอดภัยทางกายภาพ (Physical Controls) และมาตรการป้องกันที่ขับเคลื่อนด้วยเทคโนโลยี (Technological Controls)

มาตรการเหล่านี้ช่วยเสริมสร้างความแข็งแกร่งให้กับแนวทางด้านความมั่นคงปลอดภัยขององค์กร ทำให้สามารถรับมือกับภัยคุกคามทางไซเบอร์ที่เปลี่ยนแปลงไปได้อย่างมีประสิทธิภาพ พร้อมทั้งรักษาการปฏิบัติตามมาตรฐานที่เกี่ยวข้อง

นโยบายความมั่นคงปลอดภัยด้านสารสนเทศ ประกอบด้วย 4 เรื่อง ดังต่อไปนี้

4.1 มาตรการควบคุมด้านองค์กร (Organizational Controls)

บริษัทมีนโยบายและแนวทางในการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ โดยกำหนดกลยุทธ์ กระบวนการบริหารจัดการความเสี่ยง และมาตรการควบคุมที่เหมาะสม เพื่อให้การบริหารจัดการความมั่นคงปลอดภัยสารสนเทศเป็นไปอย่างมีประสิทธิภาพ และสนับสนุนการดำเนินธุรกิจอย่างต่อเนื่อง

บริษัทกำหนดบทบาทและความรับผิดชอบด้านความมั่นคงปลอดภัยสารสนเทศอย่างชัดเจน พร้อมส่งเสริมวัฒนธรรมและความตระหนักด้านความมั่นคงปลอดภัยสารสนเทศทั่วทั้งองค์กร รวมถึงมีข้อกำหนดด้านความมั่นคงปลอดภัยสารสนเทศสำหรับผู้ให้บริการ ซัพพลายเออร์ และบุคคลภายนอกที่เข้าถึงข้อมูลหรือระบบสารสนเทศของบริษัท เพื่อให้มั่นใจว่ามีการบริหารจัดการความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศตลอดความสัมพันธ์ทางธุรกิจ รวมทั้งปฏิบัติตามกฎหมาย ข้อบังคับ และมาตรฐานที่ได้รับการยอมรับ

บริษัทมุ่งมั่นทบทวน ประเมิน และปรับปรุงระบบบริหารความมั่นคงปลอดภัยสารสนเทศอย่างต่อเนื่อง เพื่อให้สามารถตอบสนองต่อความเสี่ยง ภัยคุกคาม เทคโนโลยี และข้อกำหนดที่เปลี่ยนแปลงไป พร้อมยกระดับประสิทธิภาพของมาตรการควบคุมด้านความมั่นคงปลอดภัยสารสนเทศให้สอดคล้องกับมาตรฐานที่ได้รับการยอมรับและแนวปฏิบัติที่เหมาะสมอยู่เสมอ

4.2 มาตรการควบคุมด้านบุคลากร (People Controls)

บริษัทมีนโยบายในการบริหารจัดการด้านบุคลากรเพื่อสนับสนุนความมั่นคงปลอดภัยสารสนเทศ โดยครอบคลุมการสรรหาและคัดเลือกบุคลากรที่มีคุณสมบัติเหมาะสมสำหรับตำแหน่งที่เกี่ยวข้องกับข้อมูลสำคัญ การกำหนดหน้าที่และความรับผิดชอบด้านความมั่นคงปลอดภัยสารสนเทศ รวมถึงการฝึกอบรมและการสร้างความตระหนักด้านความมั่นคงปลอดภัยสารสนเทศ เพื่อให้บุคลากรสามารถปฏิบัติหน้าที่ได้อย่างเหมาะสมและลดความเสี่ยงที่อาจเกิดขึ้น

บริษัทกำหนดให้บุคลากรทุกระดับมีบทบาท หน้าที่ และความรับผิดชอบในการปฏิบัติตามนโยบายและมาตรการด้านความมั่นคงปลอดภัยสารสนเทศ รวมถึงการปกป้องข้อมูลและระบบสารสนเทศของบริษัท พร้อมจัดให้มีมาตรการควบคุมการเข้าถึงข้อมูลและการบริหารจัดการสิทธิ์ของพนักงานอย่างเหมาะสมตั้งแต่การเริ่มงาน การเปลี่ยนตำแหน่ง จนถึงการสิ้นสุดการจ้างงาน เพื่อป้องกันการเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต และลดความเสี่ยงที่อาจเกิดขึ้นจากการละเมิดความมั่นคงปลอดภัยของข้อมูล ทั้งโดยเจตนาและไม่เจตนา

4.3 มาตรการควบคุมด้านกายภาพ (Physical Controls)

บริษัทมีนโยบายในการกำหนดมาตรการรักษาความมั่นคงปลอดภัยทางกายภาพ เพื่อปกป้องข้อมูล ทรัพย์สิน และระบบสารสนเทศจากการเข้าถึงโดยไม่ได้รับอนุญาต การโจรกรรม ความเสียหาย หรือภัยธรรมชาติที่อาจส่งผลกระทบต่อการดำเนินธุรกิจ โดยจัดให้มีมาตรการควบคุมการเข้าถึงพื้นที่ที่มีความสำคัญหรือมีข้อมูลสำคัญอย่างเหมาะสม เช่น การใช้บัตรผ่าน ระบบตรวจสอบลายนิ้วมือหรือใบหน้า กล้องโทรทัศน์วงจรปิด (CCTV) และมาตรการรักษาความปลอดภัยอื่นที่เหมาะสม เพื่อป้องกันการเข้าถึงพื้นที่โดยไม่ได้รับอนุญาต

นอกจากนี้ บริษัทต้องกำหนดมาตรการรักษาความปลอดภัยสำหรับอุปกรณ์ที่ใช้งานภายนอกองค์กร รวมถึงแนวทางในการจัดเก็บ การกำจัด หรือการทำลายข้อมูลและอุปกรณ์ที่ไม่ใช้งานแล้วอย่างเหมาะสม

เพื่อป้องกันการรั่วไหลของข้อมูล และให้การดำเนินงานเป็นไปตามนโยบายความมั่นคงปลอดภัยสารสนเทศของบริษัท

4.4 มาตรการควบคุมด้านเทคโนโลยี (Technological Controls)

บริษัทมีนโยบายในการนำมาตรการควบคุมด้านเทคโนโลยีมาใช้เพื่อปกป้องข้อมูลและระบบสารสนเทศจากภัยคุกคามทางไซเบอร์ โดยกำหนดมาตรการรักษาความมั่นคงปลอดภัยที่เหมาะสม เพื่อสนับสนุนการดำเนินธุรกิจอย่างมั่นคงและต่อเนื่อง จึงจัดให้มีมาตรการควบคุมการเข้าถึงระบบสารสนเทศ การเข้ารหัสข้อมูลที่สำคัญ การรักษาความปลอดภัยของเครือข่ายและช่องทางการสื่อสาร การบริหารจัดการช่องโหว่ การอัปเดตซอฟต์แวร์ และการสำรองข้อมูลอย่างเหมาะสม เพื่อรักษาความลับ (Confidentiality) ความถูกต้องครบถ้วน (Integrity) และความพร้อมใช้งาน (Availability) ของข้อมูลและระบบสารสนเทศตลอดวงจรชีวิตของข้อมูล รวมทั้งลดความเสี่ยงจากภัยคุกคามด้านความมั่นคงปลอดภัยสารสนเทศ

นอกจากนี้ บริษัทจัดให้มีการเฝ้าระวัง ตรวจสอบ และบันทึกเหตุการณ์ด้านความมั่นคงปลอดภัยสารสนเทศอย่างต่อเนื่อง รวมถึงมีกระบวนการตรวจจับ รายงาน ตอบสนอง และกู้คืนจากเหตุการณ์ด้านความมั่นคงปลอดภัยสารสนเทศอย่างเหมาะสมและทันท่วงที เพื่อให้สามารถลดผลกระทบจากเหตุการณ์ที่อาจเกิดขึ้น และรักษาความต่อเนื่องในการดำเนินธุรกิจ

ทั้งนี้ ให้มีผลบังคับใช้ตั้งแต่วันที่ 14 สิงหาคม 2569 เป็นต้นไป

(ดร.สุวิทย์ เมษินทรีย์)
ประธานกรรมการ