นโยบายความมั่นคงปลอดภัยไซเบอร์และเทคโนโลยีสารสนเทศ

บริษัท อมตะ วีเอ็น จำกัด (มหาชน) บริษัทร่วม บริษัทย่อยและบริษัทในเครือ (บริษัท) ตระหนักว่าข้อมูลสารสนเทศถือเป็นสินทรัพย์ที่ใช้ในการดำเนินธุรกิจที่มีค่า ซึ่งถูกจัดเก็บ รวบรวม ประมวลผล และส่งต่อผ่านระบบคอมพิวเตอร์และอุปกรณ์อิเล็กทรอนิกส์ ประกอบกับบริษัทมีนโยบายเปิดกว้างที่อนุญาตให้พนักงานใช้งานคอมพิวเตอร์ และระบบโครงข่ายเพื่อใช้งานแอพพลิเคชันและค้นหาข้อมูลโดยอิสระ ภายใต้มาตรการความปลอดภัย โดยให้ความสำคัญกับการกำกับดูแลข้อมูลสารสนเทศและไซเบอร์อย่างเป็นระบบและมีประสิทธิภาพ เพื่อป้องกันความเสี่ยงและปกป้องสินทรัพย์ รวมถึงข้อมูลสารสนเทศให้ปลอดภัยจากภัยคุกคามทางไซเบอร์ทุกรูปแบบ

บริษัทจึงได้กำหนดนโยบายนี้ขึ้น เพื่อบริหารจัดการการใช้งานคอมพิวเตอร์ ข้อมูลสารสนเทศและระบบโครงข่ายให้มั่นคง ปลอดภัยและเกิดประสิทธิภาพ โดยมุ่งเน้นการรักษาความลับ (Confidentiality) การรักษาความครบถ้วน (Integrity) ความพร้อมใช้งาน (Availability) และความมั่นคงปลอดภัย (Security) ตามกรอบมาตรฐานด้านความมั่นคงปลอดภัยไซเบอร์และเทคโนโลยีสารสนเทศทั้งในประเทศและสากล รวมถึงกฎหมาย และกฎระเบียบที่เกี่ยวข้อง เพื่อควบคุม ดูแลให้ข้อมูลและเทคโนโลยีสารสนเทศถูกนำมาใช้เพื่อสนับสนุนการดำเนินธุรกิจอย่างเหมาะสม สามารถบรรลุวัตถุประสงค์และเป้าหมายขององค์กรอย่างต่อเนื่อง

คำนิยาม

การรักษาความลับ (Confidentiality) หมายถึง การรักษาหรือสงวนไว้ เพื่อป้องกันระบบเครือข่ายคอมพิวเตอร์ ระบบคอมพิวเตอร์ ระบบสารสนเทศ ข้อมูลสารสนเทศ ข้อมูลหรืออิเล็กทรอนิกส์จากการเข้าถึง ใช้ หรือเปิดเผยโดยบุคคลที่ไม่ได้รับอนุญาต

การรักษาความครบถ้วน (Integrity) หมายถึง การดำเนินการเพื่อให้ข้อมูลสารสนเทศหรือข้อมูลอิเล็กทรอนิกส์อยู่ในสภาพสมบูรณ์ ถูกต้องและครบถ้วน ขณะที่มีการใช้งาน ประมวลผล โอน หรือเก็บรักษา เพื่อมิให้มีการเปลี่ยนแปลง แก้ไข ทำให้สูญหายหรือถูกทำลายโดยไม่ได้รับอนุญาตหรือโดยมิชอบ

ความพร้อมใช้งาน (Availability) หมายถึง การบริหารจัดการทรัพย์สินสารสนเทศขององค์กรให้สามารถทำงานได้อย่างมีประสิทธิภาพ เข้าถึงได้สะดวก รวดเร็ว หรือใช้งานได้ในเวลาที่ต้องการ

ความมั่นคงปลอดภัย (Security) หมายถึง มาตรการหรือการดำเนินการที่กำหนดขึ้นเพื่อป้องกันทรัพย์สินสารสนเทศ และรับมือ ลดความเสี่ยง ตรวจจับ และตอบสนองต่อภัยคุกคามทุกรูปแบบจากบุคคลทั้งภายในและภายนอกองค์กรที่มุ่งโจรกรรม ทำลาย ทำให้เสียหาย หรือแทรกแซงการทำงานจนเป็นเหตุให้การดำเนินธุรกิจของบริษัทได้รับความเสียหาย โดยมีหลักการดังนี้

- ความลับ (Confidentiality) การปกป้องความลับของข้อมูล โดยป้องกันการเข้าถึงและการเปิดเผยข้อมูลจากผู้ที่ไม่ได้รับอนุญาต รวมไปถึงข้อมูลส่วนบุคคลที่เป็นกรรมสิทธิ์ของบริษัท
- ความสมบูรณ์ (Integrity) การทำให้มั่นใจว่าข้อมูลของบริษัท ต้องไม่มีการแก้ไข ดัดแปลง หรือโดนทำลายโดยผู้ที่ไม่ได้รับอนุญาต
- ความพร้อมใช้งาน (Availability) การทำให้มั่นใจว่าผู้ใช้งานที่ได้รับอนุญาตสามารถเข้าถึงข้อมูลและบริการได้อย่างรวดเร็วและเชื่อถือได้
- ความรับผิดชอบ (Accountability) การระบุหน้าที่ความรับผิดชอบของแต่ละบุคคล รวมถึงการรับผิดและรับชอบในผลของการกระทำตามบทบาทหน้าที่นั้น ๆ
- การพิสูจน์ตัวจน (Authentication) การทำให้มั่นใจว่าสิทธิในการเข้าใช้งานระบบคอมพิวเตอร์และข้อมูลสารสนเทศต้องผ่านกระบวนการยืนยันตัวตนที่สมบูรณ์แล้วเท่านั้น
- การกำหนดสิทธิ (Authorization) การทำให้มั่นใจว่าการให้สิทธิเข้าใช้งานระบบคอมพิวเตอร์และข้อมูลสารสนเทศเป็นไปตามความจำเป็น (least privilege) และสอดคล้องกับความต้องการขั้นพื้นฐาน (need to know basis) ตามที่ได้รับอนุญาต
- การห้ามปฏิเสธความรับผิดชอบ (Non-repudiation) การทำให้มั่นใจว่าผู้มีส่วนร่วมที่เกี่ยวข้องในการทำธุรกรรมไม่สามารถปฏิเสธได้ว่าไม่มีส่วนเกี่ยวข้องกับการทำธุรกรรมที่เกิดขึ้น

ข้อมูล (Data) หมายถึง ข้อมูล ข้อความ คำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใดที่ถูกเก็บรักษาไว้ในรูปแบบเอกสาร สื่อสิ่งพิมพ์หรือสื่ออิเล็กทรอนิกส์ที่สามารถเข้าถึง ค้นหา หรือเรียกใช้งานผ่านระบบเครือข่ายอิเล็กทรอนิกส์ หรือเทคโนโลยีการประมวลผลข้อมูลอิเล็กทรอนิกส์ต่าง ๆ

สารสนเทศ (Information) หมายถึง ข้อมูลขององค์กรที่ผ่านการประมวลผล วิเคราะห์ คำนวณ และมีการแปลความหมายเพื่อให้ผู้ใช้เข้าใจง่าย เปรียบเทียบได้และสามารถนำไปใช้ประโยชน์ในการดำเนินงานขององค์กร ซึ่งมีลักษณะและรูปแบบที่หลากหลาย โดยรูปแบบที่พบได้ทั่วไป คือ

- ข้อมูลที่อยู่ในรูปแบบอิเล็กทรอนิกส์ เช่น เอกสารอิเล็กทรอนิกส์ ฐานข้อมูล เป็นต้น
- ข้อมูลที่ถูกจัดเก็บไว้ ซึ่งสามารถส่งต่อได้ ถอดออกได้ เครื่องมือที่ช่วยในการทำงานร่วมกัน เป็นต้น
- ข้อมูลที่อยู่ในรูปแบบเอกสารสิ่งพิมพ์ เช่น เอกสารที่พิมพ์ออกมา
- ข้อมูลที่บุคคลจดจำไปใช้

เทคโนโลยีสารสนเทศ (Information Technology) หมายถึง การประยุกต์ใช้เทคโนโลยีด้านคอมพิวเตอร์และอุปกรณ์ เครือข่ายด้านโทรคมนาคมและการสื่อสาร เพื่อค้นหา จัดเก็บ วิเคราะห์ จัดส่ง กระจายออก ติดตาม รวบรวม และจัดการข้อมูลต่าง ๆ ขององค์กร

ภัยคุกคาม (Threat) หมายถึง สถานการณ์หรือเหตุการณ์ใด ๆ ที่อาจส่งผลกระทบในทางลบต่อการปฏิบัติการหรือทรัพย์สินขององค์กร บุคคล หรือองค์กรอื่น ผ่านการเข้าถึงระบบโดยไม่ได้รับอนุญาต การทำลาย การเปิดเผย การปรับเปลี่ยนข้อมูล และ/หรือการที่ทำให้ไม่สามารถให้บริการได้

ระบบ (System) หมายถึง เครื่องมือ หรืออุปกรณ์เครือข่ายเชื่อมโยงข้อมูลและถ่ายโอนข้อมูลผ่านระบบอินเตอร์เน็ตและอินทราเน็ต ทั้งชนิดมีสายและไร้สาย รวมถึงอุปกรณ์อิเล็กทรอนิกส์และสื่อโทรคมนาคมต่าง ๆ ที่สามารถทำงานหรือใช้งานในลักษณะเดียวกัน

สินทรัพย์ (Asset) หมายถึง ข้อมูล อุปกรณ์ แอปพลิเคชัน บริการ หรือทรัพยากรด้านสารสนเทศอื่น ๆ ที่สนับสนุนการดำเนินธุรกิจ และมีมูลค่าทางเศรษฐกิจต่อองค์กร

แนวปฏิบัติ

บริษัทกำหนดแนวทางในการบริหารจัดการความมั่นคงปลอดภัยไซเบอร์และเทคโนโลยีสารสนเทศ โดยปฏิบัติตามข้อกำหนดการใช้งานคอมพิวเตอร์และระบบโครงข่ายขององค์กรที่เป็นไปตามกฎหมาย ระเบียบ มาตรฐาน และมาตรการต่าง ๆ ที่เกี่ยวข้องอย่างเคร่งครัด ซึ่งมีแนวทางที่พึงปฏิบัติ ดังนี้

1) ระบุ วิเคราะห์ ประเมินและบริหารความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์และเทคโนโลยีสารสนเทศที่สอดคล้องกับบริบททางธุรกิจและครอบคลุมความเสี่ยงที่เกิดจากผู้มีส่วนได้เสียทั้งภายในและภายนอก ตลอดห่วงโซ่อุปทาน

2) จัดทำแผนกลยุทธ์การบริหารความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์และเทคโนโลยีสารสนเทศที่เชื่อมโยงกับวิสัยทัศน์ พันธกิจ วัตถุประสงค์ และระดับความเสี่ยงที่ยอมรับได้ขององค์กร

3) กำหนดแผนหรือมาตรการรักษาความความมั่นคงปลอดภัยไซเบอร์และเทคโนโลยีสารสนเทศที่ครอบคลุมการระบุสภาพแวดล้อมและบริบททางธุรกิจ (Identify) มาตรการป้องกัน (protection) การตรวจจับเหตุการณ์ผิดปกติ (detect) การตอบสนองต่อเหตุการณ์ผิดปกติ (response) และการกู้คืน (recovery) ระบบและสินทรัพย์สารสนเทศที่ได้รับความเสียหาย

4) ดูแล ปกป้องและบริหารจัดการสินทรัพย์สารสนเทศ สถานที่ อุปกรณ์ ระบบสารสนเทศและเครือข่ายคอมพิวเตอร์ของบริษัทให้มั่นคงปลอดภัยในทุกขั้นตอนของวัฏจักรการพัฒนาระบบ

สารสนเทศ/ซอฟต์แวร์ (Secure System / Software Development Life Cycle) รวมทั้งพัฒนา บำรุงรักษาให้พร้อมใช้งานและมีประสิทธิภาพอยู่เสมอ

5) ปกป้องสารสนเทศของบริษัท ลูกค้าและคู่ค้าที่จัดเก็บ ประมวลผลหรือส่งผ่านเทคโนโลยีสารสนเทศให้ปลอดภัยจากการเข้าถึง ส่งต่อ แก้ไข ทำซ้ำ ดัดแปลง ลบ หรือทำลายโดยไม่ได้รับอนุญาต

6) จัดให้มีระบบเทคโนโลยีในการป้องกันภัยคุกคามทางไซเบอร์ และระบบรักษาความมั่นคงปลอดภัยไซเบอร์และเทคโนโลยีสารสนเทศที่มีประสิทธิภาพ ยืดหยุ่น (resilience) และสนับสนุนการทำงานที่จำเป็น

7) ตรวจประเมินช่องโหว่ (vulnerability assessment) ทดสอบการเจาะ (penetration test) รวมถึงกำหนดขั้นตอนและกระบวนการบริหารจัดการเหตุการณ์ที่อาจส่งผลกระทบต่อการรักษาความมั่นคงปลอดภัยไซเบอร์และเทคโนโลยีสารสนเทศเป็นประจำ

8) ติดตามดูแล เฝ้าระวัง และตรวจจับ (detect) เหตุการณ์ผิดปกติที่อาจส่งผลต่อความต่อเนื่องในการดำเนินธุรกิจ พร้อมทั้งบำรุงรักษาและตรวจสอบอุปกรณ์ เครือข่าย และระบบสารสนเทศให้มีประสิทธิภาพและพร้อมใช้เสมอ

9) ควบคุม จำกัดขอบเขตของผลกระทบ และดำเนินการแก้ไขให้ทันเวลา รวมทั้งปรับปรุงกระบวนการตอบสนองต่อเหตุการณ์ที่ละเมิดความมั่นคงปลอดภัยอย่างเหมาะสม สามารถป้องกัน แก้ไขและบรรเทาผลกระทบในกิจกรรมต่าง ๆ ทางธุรกิจอย่างมีประสิทธิภาพ

10) ตรวจสอบและทบทวนสถานะความปลอดภัยและกิจกรรมที่อาจส่งผลกระทบต่อเครือข่ายและระบบข้อมูลสารสนเทศขององค์กร รวมทั้งมาตรการป้องกันรักษาความมั่นคงปลอดภัยไซเบอร์และเทคโนโลยีสารสนเทศให้มีประสิทธิภาพต่อเนื่อง

11) ดำเนินการกู้คืน หรือฟื้นฟูสินทรัพย์และระบบสารสนเทศให้คืนสภาพอย่างรวดเร็ว เมื่อได้รับความเสียหายจากการถูกละเมิดความปลอดภัยของข้อมูลและการถูกคุกคามทางไซเบอร์

12) ให้การสนับสนุนและร่วมมือกับองค์กรภาคเอกชน ภาครัฐ และภาคประชาสังคมทั้งในประเทศและต่างประเทศในการป้องกันและรักษาความมั่นคงปลอดภัยไซเบอร์และเทคโนโลยีสารสนเทศ

13) จัดให้มีการสื่อสารและส่งเสริมการสร้างความตระหนักรู้ด้านการรักษาความมั่นคงปลอดภัยไซเบอร์และเทคโนโลยีสารสนเทศแก่พนักงาน คู่ค้า พันธมิตรและผู้มีส่วนได้เสียที่เกี่ยวข้อง

14) จัดให้มีช่องทางแจ้งเบาะแสและรับเรื่องร้องเรียน กระบวนการจัดการข้อร้องเรียน การคุ้มครองผู้แจ้งเบาะแสและการแจ้งผลการดำเนินการสำหรับผู้มีส่วนได้เสียทั้งภายในและภายนอกที่ได้รับผลกระทบจากการดำเนินธุรกิจของบริษัทอย่างเป็นระบบและยุติธรรม

หน้าที่ความรับผิดชอบ

เพื่อให้มั่นใจว่านโยบายความมั่นคงปลอดภัยไซเบอร์และเทคโนโลยีสารสนเทศจะได้รับการนำไปปฏิบัติอย่างทั่วถึงทั้งองค์กรและมีการกำกับดูแลที่ชัดเจน บริษัทจึงกำหนดหน้าที่ความรับผิดชอบของบุคคลหรือหน่วยงานภายในองค์กร ดังต่อไปนี้

<u>คณะกรรมการบริษัท</u>

1) พิจารณาอนุมัติและทบทวนนโยบายและมาตรการรักษาความมั่นคงปลอดภัยไซเบอร์และเทคโนโลยีสารสนเทศที่เป็นปัจจุบันเหมาะสมกับสภาพแวดล้อมและปัจจัยเสี่ยง โดยทบทวนอย่างน้อยปีละ 1 ครั้ง

2) กำกับดูแลให้การดำเนินธุรกิจสอดคล้องกับกฎหมาย ระเบียบ ข้อบังคับ นโยบายและแนวปฏิบัติที่เกี่ยวข้อง ตลอดจนส่งเสริมให้เกิดการนำนโยบายนี้ไปปฏิบัติอย่างเป็นรูปธรรม

3) กำกับดูแลและสนับสนุนให้ฝ่ายจัดการประเมินความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์และเทคโนโลยีสารสนเทศและจัดสรรทรัพยากรเพื่อให้เกิดประสิทธิผลในการควบคุมความเสี่ยงอย่างเหมาะสมและเพียงพอ

4) พิจารณารายงานเกี่ยวกับความเสี่ยงและผลการดำเนินงานตามนโยบายและมาตรการรักษาความมั่นคงปลอดภัยไซเบอร์และเทคโนโลยีสารสนเทศและให้ข้อเสนอแนะที่เป็นประโยชน์ต่อฝ่ายจัดการในการพัฒนาและปรับปรุง

5) พิจารณาประเด็นเร่งด่วนเกี่ยวกับความมั่นคงปลอดภัยไซเบอร์และเทคโนโลยีสารสนเทศเพื่อกำกับดูแลให้มีการดำเนินการที่ทันต่อสถานการณ์

6) ส่งเสริมและสนับสนุนให้ฝ่ายบริหารตระหนักและให้ความสำคัญกับการรักษาความมั่นคงปลอดภัยไซเบอร์และเทคโนโลยีสารสนเทศ และปลูกฝังให้เกิดเป็นวัฒนธรรมองค์กร

<u>ผู้บริหาร</u>

1) จัดให้มีหลักเกณฑ์ ขั้นตอนและมาตรการป้องกันที่เหมาะสมกับบริบทของแต่ละบริษัทและเป็นไปตามนโยบาย ระเบียบปฏิบัติ และกฎหมายของประเทศที่ดำเนินธุรกิจ

2) จัดให้มีโครงสร้างองค์กรที่มีผู้รับผิดชอบและบทบาทหน้าที่ที่ชัดเจน พร้อมทั้งจัดสรรทรัพยากรที่เหมาะสมและเพียงพอ

3) กำหนดกลยุทธ์และแผนการรักษาความมั่นคงปลอดภัยไซเบอร์และเทคโนโลยีสารสนเทศ รวมทั้งการบริหารความต่อเนื่องทางธุรกิจ

4) จัดให้มี พัฒนาและสอบทานระบบการบริหารความเสี่ยง การควบคุมภายใน และการตรวจสอบภายในด้านความมั่นคงปลอดภัยไซเบอร์และเทคโนโลยีสารสนเทศที่มีประสิทธิภาพ เพียงพอ

5) ติดตามดูแล บริหารจัดการและสนับสนุนให้พนักงาน คู่ค้า พันธมิตรทางธุรกิจและผู้มีส่วนได้เสียสำคัญปฏิบัติตามกฎหมาย นโยบาย มาตรการและระเบียบปฏิบัติที่เกี่ยวข้อง ตลอดจนพัฒนาปรับปรุงแนวทางปฏิบัติให้มีประสิทธิภาพยิ่งขึ้น

6) ปฏิบัติตนเป็นแบบอย่างที่ดี โดยหลีกเลี่ยงกิจกรรมใดๆ ที่อาจนำไปสู่สถานการณ์ หรือคำแนะนำที่จะทำให้เกิดการละเมิดนโยบาย

7) สนับสนุนให้ผู้ใต้บังคับบัญชาทุกระดับ ตระหนักถึงความสำคัญในการปฏิบัติตามนโยบายและปลูกฝังให้เกิดเป็นวัฒนธรรมองค์กร

8) สร้างและส่งเสริมความตระหนักรู้ และความเข้าใจด้านความมั่นคงปลอดภัยไซเบอร์และเทคโนโลยีสารสนเทศ โดยสื่อสารไปยังพนักงานและผู้มีส่วนได้เสียที่เกี่ยวข้องอย่างต่อเนื่อง

9) พิจารณารายงานผลการปฏิบัติงานตามนโยบายก่อนนำเสนอต่อคณะกรรมการ

10) จัดให้มีช่องทางแจ้งเบาะแสและรับเรื่องร้องเรียนเกี่ยวกับการละเมิดนโยบายความมั่นคงปลอดภัยไซเบอร์และเทคโนโลยีสารสนเทศ รวมทั้งกระบวนการจัดการเรื่องร้องเรียน และมาตรการคุ้มครองผู้แจ้งเบาะแส ผู้ร้องเรียน พยาน และผู้รายงานข้อมูล

<u>หน่วยงานหรือบุคคลที่รับผิดชอบความปลอดภัยไซเบอร์และเทคโนโลยีสารสนเทศ</u>

1) กำหนดขั้นตอนการปฏิบัติที่เกี่ยวข้องและมาตรการการป้องกันการละเมิดความมั่นคงปลอดภัยไซเบอร์และเทคโนโลยีสารสนเทศที่อาจเกิดขึ้น

2) กำหนดกระบวนการเปิดเผยและรายงานข้อมูลความมั่นคงปลอดภัยไซเบอร์และเทคโนโลยีสารสนเทศที่ชัดเจน

3) ประเมินและบริหารจัดการความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์และเทคโนโลยีสารสนเทศที่ครอบคลุมภัยคุกคาม (threat) ช่องโหว่ (vulnerability) ความเป็นไปได้ (likelihood) และผลกระทบ (impact) ต่อสินทรัพย์ บุคลากรขององค์กรและหน่วยงานภายนอกที่เกี่ยวข้อง รวมทั้งมีแนวทางในการป้องกันและบรรเทาผลกระทบ

4) ควบคุมภายใน บริหารจัดความเสี่ยง และติดตามตรวจสอบการปฏิบัติตามนโยบายให้มีประสิทธิภาพและรัดกุมเพียงพอ รวมทั้งแจ้งและติดตามผลกับหน่วยงานที่เกี่ยวข้อง เพื่อให้ปรับปรุงแก้ไขอย่างสม่ำเสมอ

5) ติดตาม ตรวจสอบ รวบรวมและจัดเก็บรายงานเรื่องความมั่นคงปลอดภัยไซเบอร์และเทคโนโลยีสารสนเทศ และเปิดเผยข้อมูลให้เป็นไปตามที่หน่วยงานกำกับดูแลกำหนด

6) รายงานข้อมูลความเสี่ยงหรือภัยคุกคามความมั่นคงปลอดภัยไซเบอร์และเทคโนโลยีสารสนเทศให้แก่ผู้บริหารทราบอย่างสม่ำเสมอ และรายงานในทันทีเมื่อเกิดเหตุการณ์ผิดปกติ

7) ประสานและบูรณาการความร่วมมือกับบุคคล หน่วยงานหรือผู้มีส่วนได้เสียที่เกี่ยวข้อง เพื่อร่วมกันกำหนดมาตรการ การบริหารจัดการ กลไกการควบคุม การตอบสนองและแก้ไขปัญหา

8) สื่อสารและฝึกอบรมสร้างความตระหนักรู้เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์และเทคโนโลยีสารสนเทศให้แก่พนักงานและผู้มีส่วนได้เสียที่เกี่ยวข้องอย่างต่อเนื่อง

9) ให้คำแนะนำเกี่ยวกับการดำเนินงานตามนโยบายในเบื้องต้น รวมทั้งประสานงานหรือหารือกับฝ่ายงานอื่น ๆ ที่เกี่ยวข้องในการให้คำแนะนำที่ถูกต้อง ครบถ้วนและชัดเจน

10) รายงานผลการปฏิบัติตามนโยบายต่อคณะกรรมการ ผู้บริหารหรือหน่วยงานที่เกี่ยวข้อง

11) ทบทวนนโยบายความมั่นคงปลอดภัยไซเบอร์และเทคโนโลยีสารสนเทศให้สอดคล้องกับกฎหมาย ระเบียบ แนวปฏิบัติและมาตรฐานที่เกี่ยวข้อง

<u>พนักงาน</u>

1) เรียนรู้ ทำความเข้าใจ และปฏิบัติตามตามกฎหมาย ระเบียบ ข้อบังคับ นโยบายและแนวปฏิบัติ รวมถึงมาตรฐานที่เกี่ยวข้อง

2) เมื่อพบเห็นผู้ใดกระทำผิดหรือกระทำการที่เข้าข่ายฝ่าฝืนนโยบายฉบับนี้ ให้รายงานข้อมูลหรือแจ้งข้อร้องเรียนผ่านช่องทางการแจ้งเบาะแสของบริษัท

การสื่อสารและฝึกอบรม

บริษัทจัดให้มีการสื่อสารนโยบายความมั่นคงปลอดภัยไซเบอร์และเทคโนโลยีสารสนเทศผ่านการฝึกอบรม การปฐมนิเทศ การประชุม หรือกิจกรรมในรูปแบบต่าง ๆ ที่เหมาะสมให้แก่กรรมการ ผู้บริหาร

พนักงาน บริษัทย่อย บริษัทร่วม บริษัทอื่นที่บริษัทมีอำนาจในการควบคุม ตัวแทนทางธุรกิจและคู่ค้า รวมถึงผู้มีส่วนได้เสียที่เกี่ยวข้องรับทราบ พร้อมทั้งประเมินประสิทธิผลและนำไปปรับปรุงอย่างต่อเนื่อง

การแจ้งเบาะแส

ผู้ใดพบเห็นการกระทำที่เข้าข่ายเป็นการละเมิดนโยบายนี้ให้ร้องเรียนหรือแจ้งเบาะแส โดยขั้นตอนให้เป็นไปตามนโยบายเกี่ยวกับการแจ้งเบาะแส ทั้งนี้ผู้ร้องเรียนหรือผู้แจ้งเบาะแสจะได้รับความคุ้มครองและข้อมูลจะถูกเก็บเป็นความลับ โดยไม่มีผลต่อตำแหน่งงานและค่าตอบแทน ทั้งในระหว่างดำเนินการสอบสวนและหลังเสร็จสิ้นกระบวนการ

บทลงโทษ

นโยบายความมั่นคงปลอดภัยไซเบอร์และเทคโนโลยีสารสนเทศ ถือเป็นส่วนหนึ่งของวินัยในการปฏิบัติงาน กรรมการ ผู้บริหาร และพนักงาน ผู้ที่ไม่ปฏิบัติตามย่อมถูกสอบสวนและพิจารณาโทษทางวินัยตามระเบียบของบริษัท กฎบัตร และกฎหมายที่เกี่ยวข้อง ซึ่งอาจรวมถึงการเลิกจ้าง ทั้งนี้กรณีที่เกิดการสอบสวน พนักงานทุกคนต้องให้ความร่วมมือกับหน่วยงานภายในและภายนอกอย่างเต็มที่

ในขณะเดียวกันบริษัทจะไม่ลดตำแหน่ง ลงโทษหรือให้ผลทางลบต่อกรรมการ ผู้บริหารและพนักงานที่ปฏิเสธการกระทำที่มุ่งหมายให้ละเมิดนโยบายฉบับนี้ แม้ว่าการกระทำนั้นจะทำให้บริษัทสูญเสียโอกาสทางธุรกิจ

จึงประกาศมาเพื่อทราบและถือปฏิบัติโดยทั่วกัน

ประกาศ ณ วันที่ 25 กุมภาพันธ์ 2568

(ดร.อภิชาติ ชินวรรโณ)
ประธานกรรมการ