# นโยบายการรักษาความมั่นคงปลอดภัยไซเบอร์

เพื่อให้กลุ่มมิตรผลสามารถบริหารงานได้อย่างมีประสิทธิภาพ สอดคล้องกับนโยบายด้านเทคโนโลยีสารสนเทศของกลุ่มมิตรผล พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ.2562 พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.2550 พระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ.2544 รวมถึงกฎหมาย ระเบียบ ข้อบังคับอื่นที่เกี่ยวข้อง จึงกำหนดนโยบายการรักษาความมั่นคงปลอดภัยไซเบอร์ของกลุ่มมิตรผล ดังต่อไปนี้

## 1. วัตถุประสงค์

การรักษาความปลอดภัยไซเบอร์ของระบบสารสนเทศที่ใช้งานภายในบริษัทเป็นสิ่งสำคัญที่จะต้องมีการคำนึงถึง เนื่องจากมีหลายปัจจัยที่อาจก่อให้เกิดภัยคุกคามได้ เช่น บุคคลผู้ไม่ประสงค์ดีสามารถดำเนินการได้จากที่ใดก็ได้ ช่องโหว่จากการเชื่อมต่อระหว่างระบบสารสนเทศ ความสามารถในการปิดและแก้ไขช่องโหว่ของระบบสารสนเทศที่มีความซับซ้อน เป็นต้น โดยเหตุการณ์ภัยคุกคามดังกล่าวอาจกระทบการดำเนินธุรกิจของบริษัทหรือกระทบต่อสิทธิและเสรีภาพของเจ้าของข้อมูลส่วนบุคคล อันประกอบด้วย พนักงาน ลูกค้า และกลุ่มบุคคลอื่นที่เกี่ยวข้องที่กลุ่มมิตรผลได้มีการประมวลผลข้อมูลส่วนบุคคล ดังนั้นการปฏิบัติตามนโยบายฉบับนี้จึงเป็นสิ่งสำคัญที่จะช่วยลดความเสี่ยงทางไซเบอร์ได้

นโยบายฉบับนี้ ได้มีการกำหนดถึงการปกป้องทรัพย์สินสารสนเทศ การติดตาม และการกำกับดูแลหน่วยงานด้านเทคโนโลยีสารสนเทศในการบริหารจัดการระบบสารสนเทศและการประมวลผลข้อมูลให้มีความมั่นคงปลอดภัยจากภัยคุกคามทางไซเบอร์ และครอบคลุมถึงหน่วยงานทางธุรกิจที่ได้ดำเนินการบริหารจัดการระบบสารสนเทศและประมวลผลข้อมูลเองโดยไม่ผ่านการควบคุมดูแลจากหน่วยงานด้านเทคโนโลยีสารสนเทศ ซึ่งจะต้องปฏิบัติตามนโยบายฉบับนี้อย่างเคร่งครัด

## 2. คำจำกัดความ

**ระบบสารสนเทศ (Information System)** หมายถึง ระบบงานคอมพิวเตอร์ ระบบการสื่อสาร ระบบข้อมูลต่างๆ ที่มีการบันทึกประมวลผล เรียกดู หรือมีการโอนย้ายผ่านระบบดังกล่าว รวมถึง โปรแกรม ข้อกำหนดของระบบและกระบวนการต่าง ๆ ที่ใช้ในการปฏิบัติงานและการบำรุงรักษาระบบ

**การรักษาความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity)** หมายถึง มาตรการหรือการดำเนินการที่กำหนดขึ้นเพื่อป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ทั้งจากภายในและภายนอกบริษัท

**ภัยคุกคามไซเบอร์ (Cyber Threat)** หมายถึง การกระทำหรือการดำเนินการใดๆ โดยมิชอบ โดยใช้คอมพิวเตอร์หรือระบบคอมพิวเตอร์หรือโปรแกรมไม่พึงประสงค์โดยมุ่งหมายให้เกิดการประทุษร้ายต่อระบบคอมพิวเตอร์ ข้อมูลคอมพิวเตอร์ หรือข้อมูลอื่นที่เกี่ยวข้อง

**การรักษาความลับ (Confidentiality)** หมายถึง การรักษาหรือสงวนไว้เพื่อป้องกันระบบเครือข่ายคอมพิวเตอร์ ระบบคอมพิวเตอร์ ระบบงานคอมพิวเตอร์ ระบบสารสนเทศ ข้อมูลสารสนเทศ ข้อมูลอิเล็กทรอนิกส์ หรือข้อมูลคอมพิวเตอร์ จากการเข้าถึง การใช้ หรือเปิดเผย โดยบุคคลซึ่งไม่ได้รับอนุญาต

**การรักษาความครบถ้วน (Integrity)** หมายถึง การดำเนินการเพื่อให้ข้อมูลสารสนเทศ ข้อมูลอิเล็กทรอนิกส์ หรือข้อมูลคอมพิวเตอร์อยู่ในสภาพสมบูรณ์ ขณะที่มีการใช้งาน ประมวลผล โอน หรือเก็บรักษา เพื่อมิให้มีการเปลี่ยนแปลงแก้ไข ทำให้สูญหาย ทำให้เสียหาย หรือถูกทำลาย โดยไม่ได้รับอนุญาตหรือโดยมิชอบ

**การรักษาสภาพพร้อมใช้งาน (Availability)** หมายถึง การจัดทำให้ทรัพย์สินสารสนเทศหรือเทคโนโลยีสารสนเทศสามารถทำงาน เข้าถึง หรือใช้งานได้ในเวลาที่ต้องการ

**มาตรฐาน (Standard)** หมายถึง บรรทัดฐานที่บังคับใช้ในการปฏิบัติงานจริง เพื่อให้ได้ตามวัตถุประสงค์หรือเป้าหมาย

**ระเบียบปฏิบัติ (Procedure)** หมายถึง กระบวนการที่กำหนดขึ้นเพื่อใช้ในการปฏิบัติงานหรือตอบสนองในสถานการณ์ที่กำหนด เพื่อให้บรรลุถึงวัตถุประสงค์ของการบริหารงาน และเป็นการนำนโยบายไปปฏิบัติเพื่อให้เกิดผลบังคับใช้ กระบวนการปฏิบัติงานดังกล่าวต้องมีผลบังคับใช้เสมอจนกว่าจะมีการอนุมัติยกเว้นเป็นลายลักษณ์อักษร

**กรอบการบริหารจัดการด้านความมั่นคงปลอดภัยไซเบอร์** หมายถึง กรอบที่ใช้ในการบริหารจัดการและการควบคุมด้านไซเบอร์ ซึ่งกำหนดขึ้นโดย National Institute of Standards and Technology (NIST) ซึ่งอ้างอิงเวอร์ชัน 1.1 (NIST Cybersecurity Framework v1.1)

**กรอบการบริหารจัดการด้านข้อมูลส่วนบุคคล** หมายถึง กรอบที่ใช้ในการบริหารจัดการและการควบคุมด้านข้อมูลส่วนบุคคล ซึ่งกำหนดขึ้นโดย National Institute of Standards and Technology (NIST) ซึ่งอ้างอิงเวอร์ชัน 1.0 (NIST Privacy Framework v1.0)

**มาตรการควบคุม (Control)** หมายถึง วิธีการบริหารจัดการความเสี่ยง ซึ่งหมายรวมถึงนโยบาย ขั้นตอนการปฏิบัติงาน แนวทางปฏิบัติงาน วิธีการทำงาน หรือโครงสร้างบริษัท ทั้งที่อยู่ในเชิงการควบคุมดูแล เทคนิคการบริหารจัดการ หรือกฎหมาย

**การประเมินความเสี่ยง (Risk Assessment)** หมายถึง กระบวนการในการระบุระดับความรุนแรงและการจัดลำดับความสำคัญของปัจจัยเสี่ยงโดยประเมินจากโอกาสที่จะเกิดขึ้น (Likelihood) และผลกระทบ (Impact) ที่จะเกิดขึ้น

**การพิสูจน์ตัวตน (Authentication)** หมายถึง การประมวลผลโดยระบบคอมพิวเตอร์ เพื่อตรวจสอบและรับรองตัวตนของผู้ใช้ โดยตรวจสอบจากรหัสบัญชีผู้ใช้และรหัสผ่านก่อนการอนุญาตให้เข้าถึงทรัพยากรต่างๆ ในระบบ เช่น คีย์การ์ด (Key Card) รหัสผ่าน (Password) หรือการใช้พิน (PINs) ลายนิ้วมือ (Finger print) เป็นต้น

**ความปลอดภัยทางกายภาพ (Physical Security)** หมายถึง การควบคุมความปลอดภัยด้านกายภาพของการเข้าถึงข้อมูล ที่มีผลต่อความต่อเนื่องในการปฏิบัติงานในระบบคอมพิวเตอร์หรือทรัพย์สินสารสนเทศที่มีค่าของบริษัท

**การใช้บริการจากหน่วยงานภายนอก (External Party Services)** หมายถึง บริการที่บริษัทใช้หรือได้รับจากผู้ให้บริการภายนอก เช่น การใช้บริการเก็บรักษาข้อมูล การใช้บริการประมวลผลข้อมูล การใช้บริการจากผู้จัดจำหน่ายฮาร์ดแวร์และซอฟต์แวร์ ผู้ให้คำปรึกษาทางด้านธุรกิจและด้านความปลอดภัย รวมถึงประเภทของการใช้บริการอื่นที่ไม่ได้ให้บริการอยู่ภายในบริษัทด้วย เช่น การใช้บริการด้านอินเทอร์เน็ตและระบบเครือข่ายงานที่เชื่อมต่อกันทั่วโลก

**ข้อมูลสารสนเทศ (Information)** หมายถึง ข้อมูลทั้งที่อยู่ในรูปแบบเอกสารและข้อเท็จจริงที่อยู่ในรูปแบบต่างๆ เช่น ข้อมูลที่อยู่ในแบบฟอร์มบริษัท รวมถึงที่อยู่ในระบบสารสนเทศ ระบบเครือข่าย อุปกรณ์คอมพิวเตอร์ หรือสื่อในการจัดเก็บข้อมูลของบริษัท ไม่ว่าข้อมูลเหล่านี้จะอยู่ในรูปแบบใดๆ เช่น ในรูปแบบของเอกสารที่จัดพิมพ์ เทปแม่เหล็กไมโครฟิช (Microfiche) ข้อมูลออนไลน์ เป็นต้น

**ผู้ควบคุมข้อมูล (Data Controller)** หมายถึง ผู้บริหารของหน่วยงานทางธุรกิจที่ทำหน้าที่รับผิดชอบต่อการสร้างข้อมูล ใช้ข้อมูล หรือให้ความเชื่อถือได้ของข้อมูล

**ผู้ประมวลผลข้อมูล (Data Processor)** หมายถึง ผู้บริหารของหน่วยงานทางธุรกิจที่ทำหน้าที่รับผิดชอบในการบริหารจัดการการประมวลผลข้อมูล โดยข้อมูลจะอยู่ภายใต้การกำกับดูแลและบริหารจัดการโดยผู้ควบคุมข้อมูล

**เจ้าของข้อมูลส่วนบุคคล (Data Subject)** หมายถึง ตัวบุคคลที่เป็นเจ้าของข้อมูลส่วนบุคคล โดยไม่ใช่เป็นผู้ที่ครอบครองข้อมูล หรือเป็นผู้สร้าง หรือเก็บรวบรวมข้อมูลนั้นเอง โดยเจ้าของข้อมูลส่วนบุคคลจะหมายถึงบุคคลธรรมดาเท่านั้น และไม่รวมถึงนิติบุคคล

**ทรัพย์สินสารสนเทศ (Information Asset)** หมายถึง สิ่งที่มีคุณค่าหรือมูลค่าต่อบริษัท โดยอาจเป็นทรัพย์สินสารสนเทศที่เกี่ยวข้องกับการประมวลผลสารสนเทศที่บริษัทเป็นเจ้าของ เช่า ว่าจ้าง พัฒนา หรือจัดซื้อ เพื่อประโยชน์ในการดำเนินธุรกิจหรือการปฏิบัติงานของบริษัท ซึ่งทรัพย์สินสารสนเทศมีได้หลายประเภท ดังนี้

- ทรัพย์สินสารสนเทศที่มีตัวตน (Tangible Information Asset) เช่น อุปกรณ์คอมพิวเตอร์ อุปกรณ์การติดต่อสื่อสาร สื่อบันทึกข้อมูล และอุปกรณ์อื่นที่เกี่ยวข้องกับการประมวลผลสารสนเทศ เป็นต้น
- ทรัพย์สินสารสนเทศที่ไม่มีตัวตน (Intangible Information Asset)
  - **สารสนเทศ (Information)** เช่น ฐานข้อมูลและไฟล์ข้อมูล สัญญาและข้อตกลงต่างๆ เอกสาร คู่มือระบบงาน ข้อมูลวิจัย ไฟล์คู่มือผู้ใช้งาน ไฟล์เอกสารการฝึกอบรม ขั้นตอนการปฏิบัติงาน แผนรองรับความต่อเนื่อง ทางธุรกิจ (BCP Plan) ข้อตกลงในการถอยกลับ (Fallback Arrangement) เอกสารหรือเร็คคอร์ดเพื่อการตรวจสอบ (Audit Trail) ข้อมูลที่ถูกจัดเก็บถาวร เป็นต้น
  - **ซอฟต์แวร์ (Software Asset)** เช่น ซอฟต์แวร์ระบบงาน(Application Software) ซอฟต์แวร์ระบบปฏิบัติการคอมพิวเตอร์ (Operating System) เครื่องมือในการพัฒนาระบบงาน (Software Development Tools) เป็นต้น

**การเข้ารหัส (Encryption)** หมายถึง การนำข้อมูลมาเข้ารหัสลับเพื่อป้องกันการลักลอบเข้ามาใช้ข้อมูล ผู้ที่สามารถเปิดไฟล์ข้อมูลที่เข้ารหัสลับไว้จะต้องมีโปรแกรมถอดรหัสลับเพื่อให้ข้อมูลกลับมาใช้งานได้ตามปกติ

**การปฏิบัติงานภายนอกสำนักงาน (Remote Working)** หมายถึง การเชื่อมต่อเข้าสู่เครือข่ายของบริษัทจากอุปกรณ์ที่เชื่อมต่อผ่านเครือข่ายภายนอกบริษัท

**ช่องโหว่ด้านความปลอดภัยสารสนเทศ (Vulnerability)** หมายถึง จุดอ่อนด้านความปลอดภัยสารสนเทศที่ภัยคุกคามสามารถใช้ประโยชน์ ซึ่งอาจทำให้เกิดความเสียหายต่อระบบสารสนเทศ ข้อมูล และข้อมูลส่วนบุคคล หรือการดำเนินธุรกิจของบริษัท

## 3. บทบาทความรับผิดชอบ

3.1. คณะกรรมการบริษัทเป็นผู้กำหนดทิศทางและสนับสนุนการนำนโยบายการรักษาความมั่นคงปลอดภัยไซเบอร์ไปปฏิบัติในกลุ่มมิตรผล ผ่านทางคณะกรรมการความปลอดภัยทางไซเบอร์และประธานเจ้าหน้าที่บริหาร

3.2. คณะกรรมการความปลอดภัยทางไซเบอร์เป็นผู้พิจารณากลั่นกรอง ให้คำแนะนำเกี่ยวกับความเสี่ยงและความเพียงพอของมาตรการรักษาความมั่นคงปลอดภัยไซเบอร์ โดยประสานงานกับคณะกรรมการความเสี่ยงและรายงานให้คณะกรรมการบริษัททราบเป็นระยะ

3.3. ฝ่ายจัดการ

3.3.1. หน่วยงานด้านความมั่นคงปลอดภัยไซเบอร์เป็นผู้นำนโยบายไปปฏิบัติ ชี้แจงและสื่อสารไปยังผู้ที่เกี่ยวข้อง กำกับดูแล ติดตามความเสี่ยงและความเพียงพอของมาตรการรักษาความมั่นคงปลอดภัยไซเบอร์ให้สอดคล้องกับการบริหารความเสี่ยงระดับองค์กร โดยได้รับการสนับสนุนจากคณะกรรมการความปลอดภัยทางไซเบอร์

3.3.2. หน่วยงานอื่นๆ เป็นผู้ควบคุมดูแลให้มีการนำนโยบายไปปฏิบัติ ชี้แจงและสื่อสารไปยังผู้ที่เกี่ยวข้องและติดตามการนำไปปฏิบัติอย่างต่อเนื่อง โดยได้รับการสนับสนุนจากคณะกรรมการความปลอดภัยทางไซเบอร์และหน่วยงานด้านความมั่นคงปลอดภัยไซเบอร์

3.4. พนักงานทุกคนให้ปฏิบัติตามนโยบายการรักษาความมั่นคงปลอดภัยไซเบอร์ รวมถึงแนวปฏิบัติและขั้นตอนปฏิบัติงานที่เกี่ยวข้องที่ได้รับการอนุมัติอย่างเคร่งครัด

## 4. หลักสำคัญในการปฏิบัติ

4.1. การกำกับดูแลและการบริหารจัดการความมั่นคงปลอดภัยไซเบอร์ บริษัทมีมาตรการหรือวิธีการดำเนินงานเพื่อให้มั่นใจว่ามีการกำกับดูแลและบริหารจัดการความมั่นคงปลอดภัยไซเบอร์อย่างมีประสิทธิผล ครอบคลุมทั้งบริษัทและเป็นไปตามข้อกฎหมายที่เกี่ยวข้อง

4.2. กรอบการบริหารจัดการด้านความมั่นคงปลอดภัยไซเบอร์ บริษัทมีมาตรการหรือวิธีการดำเนินงานเพื่อให้มั่นใจว่ามีการกำหนดแนวปฏิบัติในการบริหารจัดการด้านความมั่นงปลอดภัยไซเบอร์และข้อมูล

ส่วนบุคคล โดยยึดตามหลักมาตรฐานสากลขององค์กร National Institute of Standards and Technology (NIST) ซึ่งประกอบด้วย กรอบการบริหารจัดการด้านความมั่นคงปลอดภัยไซเบอร์ (NIST Cybersecurity Framework) และกรอบการบริหารจัดการด้านข้อมูลส่วนบุคคล (NIST Privacy Framework)

4.3. การบริหารความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ บริษัทมีมาตรการหรือวิธีการดำเนินงานเพื่อให้มั่นใจว่ามีการประเมินความเสี่ยงและการควบคุมด้านความมั่นคงปลอดภัยไซเบอร์และข้อมูลส่วนบุคคล รวมถึงมีการจัดการความเสี่ยงให้อยู่ในระดับที่องค์กรยอมรับได้ ตลอดจนมีการติดตามและรายงานความเสี่ยงอย่างสม่ำเสมอ โดยสอดคล้องกับการบริหารความเสี่ยงระดับองค์กรและมาตรฐานสากล

4.4. การบริหารจัดการทรัพย์สินด้านเทคโนโลยีสารสนเทศ บริษัทมีมาตรการหรือวิธีการดำเนินงานเพื่อให้มั่นใจว่ามีการจัดทำทะเบียนรายการทรัพย์สินด้านเทคโนโลยีสารสนเทศอย่างครบถ้วน และควบคุมดูแลทรัพย์สินด้านเทคโนโลยีสารสนเทศให้มีความพร้อมใช้งานและสามารถรองรับการให้บริการหรือดำเนินธุรกิจได้อย่างต่อเนื่อง โดยครอบคลุมถึงการควบคุมให้เกิดการใช้งานทรัพย์สินด้านเทคโนโลยีสารสนเทศอย่างเหมาะสม และถูกต้องตามลิขสิทธิ์

4.5. การบริหารจัดการทรัพยากรบุคคลเพื่อความมั่นคงปลอดภัยไซเบอร์ บริษัทมีมาตรการหรือวิธีการดำเนินงานเพื่อให้มั่นใจว่ามีการสื่อสารไปยังผู้บริหาร พนักงาน ลูกจ้าง และบุคคลที่ปฏิบัติหน้าที่ให้กับบริษัทรับทราบและเข้าใจบทบาทหน้าที่ในการปฏิบัติตามนโยบายการรักษาความมั่นคงปลอดภัยไซเบอร์ รวมถึงแนวปฏิบัติที่เกี่ยวข้อง

4.6. การบริหารจัดการความมั่นคงปลอดภัยด้านกายภาพและสภาพแวดล้อม บริษัทมีมาตรการหรือวิธีการดำเนินงานเพื่อให้มั่นใจว่ามีการรักษาความมั่นคงปลอดภัยและความพร้อมใช้งานของศูนย์คอมพิวเตอร์และพื้นที่สำคัญที่เกี่ยวข้องกับระบบเทคโนโลยีสารสนเทศอย่างเพียงพอ และสามารถรองรับความต้องการของธุรกิจได้อย่างต่อเนื่อง

4.7. การรักษาความมั่นคงปลอดภัยของข้อมูลสารสนเทศ บริษัทมีมาตรการหรือวิธีการดำเนินงานเพื่อให้มั่นใจว่ามีการรักษาความมั่นคงปลอดภัยของข้อมูลทั้งในรูปแบบกระดาษและอิเล็กทรอนิกส์ ครอบคลุมถึงการรับส่งข้อมูลผ่านระบบเครือข่ายสื่อสาร การจัดเก็บ การใช้ข้อมูลบนระบบงาน สื่อบันทึกข้อมูลต่างๆ การเก็บรักษา และการทำลายข้อมูล

4.8. การบริหารจัดการการเข้าถึง บริษัทมีมาตรการหรือวิธีการดำเนินงานเพื่อให้มั่นใจว่ามีการควบคุมการเข้าถึงระบบปฏิบัติการ ระบบเครือข่าย ระบบเทคโนโลยีสารสนเทศ และระบบฐานข้อมูล โดยกำหนดให้มีการบริหารจัดการสิทธิและตรวจสอบยืนยันตัวตนตามสิทธิที่กำหนดไว้ตามความจำเป็นในการใช้งานและระดับความเสี่ยง เพื่อป้องกันการเข้าถึงและเปลี่ยนแปลงระบบหรือข้อมูลโดยผู้ที่ไม่มีสิทธิหรือไม่ได้รับอนุญาต ตามหลักความจำเป็นของการใช้งาน (Least Privilege) และสอดคล้องกับหลักการแบ่งแยกงานด้านเทคโนโลยีสารสนเทศที่ดี (Segregation of Duties)

4.9. การจัดหา การพัฒนา และการบำรุงรักษาระบบ บริษัทมีมาตรการหรือวิธีการดำเนินงานเพื่อให้มั่นใจว่ามีการจัดหา การพัฒนา และการบำรุงรักษาระบบ มีการควบคุมการรักษาความปลอดภัยอย่างรัดกุมและสอดคล้องตามหลักการควบคุมที่เป็นมาตรฐานสากล

4.10. การตรวจสอบช่องโหว่และการทดสอบเจาะระบบ บริษัทมีมาตรการหรือวิธีการดำเนินงานเพื่อให้มั่นใจว่ามีการดำเนินการเพื่อให้ได้รับทราบถึงช่องโหว่ด้านการรักษาความปลอดภัยของระบบ และสามารถดำเนินการปรับปรุงแก้ไขป้องกันความเสี่ยงจากภัยคุกคามใหม่ ๆ ที่อาจเกิดขึ้นได้อย่างทันการณ์

4.11. การเฝ้าระวังเหตุการณ์ผิดปกติด้านความมั่นคงปลอดภัยไซเบอร์ บริษัทมีมาตรการหรือวิธีการดำเนินงานเพื่อให้มั่นใจว่ามีการดำเนินการเพื่อให้สามารถตรวจจับ ป้องกัน และรับมือเหตุการณ์ผิดปกติได้อย่างทันท่วงที โดยมีกระบวนการติดตามดูแลความมั่นคงปลอดภัยของระบบ รวมถึงเฝ้าระวังภัยคุกคามอย่างต่อเนื่อง

4.12. การบริหารจัดการเหตุการณ์ผิดปกติด้านความมั่นคงปลอดภัยไซเบอร์ บริษัทมีมาตรการหรือวิธีการดำเนินงานเพื่อให้มั่นใจว่ามีการบริหารจัดการเหตุการณ์ผิดปกติจากภัยคุกคามทางไซเบอร์ ซึ่งรวมถึงเหตุการณ์ผิดปกติด้านเทคโนโลยีสารสนเทศอย่างเหมาะสมทันการณ์ เพื่อให้สามารถจัดการแก้ไขปัญหาให้กลับสู่สภาพปกติได้อย่างรวดเร็วและจำกัดความเสียหายที่ส่งผลกระทบต่อการดำเนินธุรกิจของบริษัท

4.13. การบริหารจัดการผู้ให้บริการภายนอก บริษัทมีมาตรการหรือวิธีการดำเนินงานเพื่อให้มั่นใจว่ามีการบริหารจัดการความเสี่ยงจากการใช้บริการ การเชื่อมต่อ หรือการเข้าถึงข้อมูลจากบุคคลภายนอกให้มีความเสี่ยงในระดับที่บริษัทยอมรับได้

4.14. การบริหารจัดการความต่อเนื่องทางธุรกิจ บริษัทมีมาตรการหรือวิธีการดำเนินงานเพื่อให้มั่นใจว่ามีการรองรับเหตุการณ์ผิดปกติที่ทำให้ระบบเกิดหยุดชะงักหรือเกิดความเสียหาย โดยที่ธุรกิจสามารถดำเนินการต่อไปได้อย่างต่อเนื่อง และสามารถกู้คืนระบบให้กลับคืนสู่สภาพปกติภายในระยะเวลาที่ยอมรับได้

4.15. กฎหมายและข้อบังคับที่เกี่ยวข้อง บริษัทมีมาตรการหรือวิธีการดำเนินงานเพื่อให้มั่นใจว่ามีการดำเนินการ เพื่อป้องกันการละเมิดข้อผูกพันในกฎหมาย ระเบียบ ข้อบังคับ หรือสัญญาจ้างที่เกี่ยวข้อง

กับพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล รวมถึงกฎหมาย ระเบียบ ข้อบังคับอื่นที่เกี่ยวข้อง ซึ่งใช้บังคับอยู่แล้วในขณะนี้และที่จะออกใช้บังคับต่อไปในภายหน้า

## 5. การทบทวนนโยบาย

5.1. ในกรณีที่ฝ่ายจัดการพบว่านโยบายการรักษาความมั่นคงปลอดภัยไซเบอร์ฉบับนี้ไม่เหมาะสมกับสภาพแวดล้อมการดำเนินธุรกิจ หรือ มีการเปลี่ยนแปลงที่มีนัยสำคัญต่างๆ ต่อกฎเกณฑ์ กฎหมาย และ เทคโนโลยี ที่ส่งผลกระทบต่อบริษัท ต้องนำเสนอต่อคณะกรรมการบริษัท ผ่านคณะกรรมการความปลอดภัยทางไซเบอร์ เพื่อขออนุมัติปรับปรุง

5.2. คณะกรรมการความปลอดภัยทางไซเบอร์ จะทบทวนนโยบายการรักษาความมั่นคงปลอดภัยไซเบอร์ฉบับนี้เป็นประจำทุกปีและนำเสนอต่อคณะกรรมการบริษัท เพื่อให้มั่นใจว่านโยบายดังกล่าวยังเหมาะสมกับสภาพแวดล้อมการดำเนินธุรกิจของกลุ่มมิตรผล

ประธานกรรมการบริษัท กลุ่มมิตรผล

นายบรรเทิง ว่องกุศลกิจ