นโยบายการกำกับดูแลและบริหารจัดการเทคโนโลยีสารสนเทศ

(IT Governance Policy)

Enterprise IT Governance Office

บริษัท กรุงเทพดุสิตเวชการ จำกัด (มหาชน) | 2 ซอยศูนย์วิจัย 7 ถนนเพชรบุรีตัดใหม่ แขวงบางกะปิ เขตห้วยขวาง กรุงเทพมหานคร 10310

สารบัญ

นโยบายการกำกับดูแลและบริหารจัดการเทคโนโลยีสารสนเทศ

(IT Governance Policy)

ในยุคที่เทคโนโลยีสารสนเทศมีบทบาทสำคัญในการขับเคลื่อนการดำเนินงานขององค์กร ทั้งในด้านการให้บริการ การบริหารจัดการข้อมูล และการสนับสนุนกระบวนการตัดสินใจเชิงกลยุทธ์ บริษัทตระหนักถึงความจำเป็นในการมีระบบการกำกับดูแลและบริหารจัดการเทคโนโลยีสารสนเทศที่มีความมั่นคง ปลอดภัย โปร่งใส และสามารถตอบสนองต่อการเปลี่ยนแปลงของสภาพแวดล้อมทางธุรกิจได้อย่างมีประสิทธิภาพ โดยเฉพาะในบริบทของธุรกิจด้านสุขภาพ ซึ่งมีการจัดการข้อมูลส่วนบุคคลและข้อมูลสุขภาพที่มีความอ่อนไหวสูง และมีการประยุกต์ใช้เทคโนโลยีดิจิทัลและปัญญาประดิษฐ์ (AI) ในกระบวนการทางคลินิกและธุรกิจ การกำกับดูแลเทคโนโลยีสารสนเทศอย่างรัดกุมจึงเป็นองค์ประกอบสำคัญในการสร้างความเชื่อมั่น ความปลอดภัย และความสอดคล้องต่อกฎหมาย กฎระเบียบ และมาตรฐานสากลที่เกี่ยวข้อง

ด้วยเหตุนี้ คณะกรรมการและฝ่ายบริหารของบริษัท กรุงเทพดุสิตเวชการ จำกัด (มหาชน) จึงได้จัดทำนโยบายฉบับนี้ขึ้น เพื่อกำหนดกรอบแนวทางในการกำกับดูแลและบริหารจัดการเทคโนโลยีสารสนเทศขององค์กรให้ครอบคลุมทั้งด้านโครงสร้างการบริหารจัดการ บทบาทหน้าที่ของหน่วยงานที่เกี่ยวข้อง แนวทางการจัดการความเสี่ยง การคุ้มครองข้อมูล ตลอดจนการใช้เทคโนโลยีเกิดใหม่ (Emerging Technology) อย่างมีธรรมาภิบาล เพื่อให้การดำเนินงานขององค์กรมีความยั่งยืน ปลอดภัย และสามารถสร้างคุณค่าทางธุรกิจในระยะยาวได้อย่างแท้จริง

1. **วัตถุประสงค์** (Purpose)

นโยบายฉบับนี้จัดทำขึ้นเพื่อกำหนดกรอบแนวทางการกำกับดูแลและบริหารจัดการเทคโนโลยีสารสนเทศขององค์กรให้เป็นไปอย่างมีประสิทธิภาพ โปร่งใส ตรวจสอบได้ และสอดคล้องกับเป้าหมายทางธุรกิจ กฎหมายที่เกี่ยวข้อง และมาตรฐานสากลด้านความมั่นคงปลอดภัยสารสนเทศ โดยมีวัตถุประสงค์หลัก ดังนี้

1.1 กำหนดโครงสร้างการกำกับดูแลด้านเทคโนโลยีสารสนเทศที่ชัดเจน ครอบคลุม และมีความรับผิดชอบร่วมกันในทุกระดับขององค์กร

1.2 สร้างกลไกการบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศที่มีประสิทธิภาพ เพื่อป้องกันผลกระทบที่อาจเกิดขึ้นต่อความต่อเนื่องทางธุรกิจ ชื่อเสียงขององค์กร และความเชื่อมั่นของผู้รับบริการ

1.3 ส่งเสริมการใช้เทคโนโลยีสารสนเทศและปัญญาประดิษฐ์ (Artificial Intelligence: AI) อย่างมีจริยธรรม มีความมั่นคงปลอดภัย และอยู่ภายใต้การควบคุมที่เหมาะสม

1.4 สนับสนุนการปฏิบัติตามกฎหมาย กฎระเบียบ และข้อกำหนดของหน่วยงานกำกับดูแลที่เกี่ยวข้อง

1.5 เสริมสร้างวัฒนธรรมองค์กรด้านการกำกับดูแลเทคโนโลยี (Technology Governance Culture) ให้บุคลากรทุกระดับมีความตระหนักและปฏิบัติตามแนวทางที่กำหนดอย่างสม่ำเสมอ

2. **ขอบเขต** (Scope)

นโยบายฉบับนี้ครอบคลุมถึงการกำกับดูแลและบริหารจัดการด้านเทคโนโลยีสารสนเทศ ระบบดิจิทัล และระบบปัญญาประดิษฐ์ (Artificial Intelligence: AI) รวมถึงแนวท1างในการบริหารความเสี่ยง ความมั่นคงปลอดภัยของข้อมูล การคุ้มครองข้อมูลส่วนบุคคลและข้อมูลสุขภาพ การบริหารจัดการผู้ให้บริการภายนอก (Third Party Management) และการปฏิบัติตามกฎหมายและข้อกำหนดที่เกี่ยวข้อง

โดยนโยบายฉบับนี้ถือเป็นข้อกำหนดที่มีผลบังคับใช้กับคณะกรรมการ ผู้บริหารและพนักงานในกลุ่มธุรกิจของบริษัท กรุงเทพดุสิตเวชการ จำกัด (มหาชน) บริษัทย่อยและกิจการอื่น ๆ ที่บริษัทมีอำนาจควบคุมการดำเนินการ (รายละเอียดดังเอกสารแนบท้าย 1) โดยไม่มีข้อยกเว้น และรวมถึงคู่สัญญาหรือผู้ให้บริการที่เข้ามาดำเนินงานร่วมกับองค์กร โดยทุกฝ่ายจะต้องยึดถือและปฏิบัติตามนโยบายนี้อย่างเคร่งครัด เพื่อให้การใช้เทคโนโลยีสารสนเทศและดิจิทัลภายในองค์กรเป็นไปอย่างมีประสิทธิภาพ ปลอดภัย โปร่งใส และสอดคล้องกับเป้าหมายทางธุรกิจหรือพันธกิจขององค์กร

1. คณะกรรมการบริษัท คณะกรรมการชุดย่อย และผู้บริหารระดับสูงที่เกี่ยวข้องกับการกำหนดทิศทาง เชิงกลยุทธ์ในการบริหารเทคโนโลยีสารสนเทศและการกำกับดูแลให้หน่วยงานดำเนินงานตามนโยบายด้านเทคโนโลยีสารสนเทศ
2. พนักงานและบุคลากรทุกระดับ รวมถึงผู้ปฏิบัติงานที่มีหน้าที่ใช้ระบบสารสนเทศหรือบริหารจัดการระบบเทคโนโลยีสารสนเทศ
3. หน่วยงานภายในทั้งหมดที่เกี่ยวข้องกับการใช้ การพัฒนา หรือการบริหารจัดการระบบเทคโนโลยีและข้อมูลสารสนเทศ
4. คู่ค้า ผู้ให้บริการภายนอก พันธมิตรทางธุรกิจ กิจการร่วมค้า และบุคคลที่เกี่ยวข้องกับการดำเนินงานด้านเทคโนโลยีสารสนเทศและดิจิทัลขององค์กร ภายใต้ข้อกำหนดด้านความมั่นคงปลอดภัยตามที่องค์กรระบุไว้ในสัญญาหรือความร่วมมือ

นโยบายนี้ให้ใช้บังคับควบคู่กับระเบียบ ประกาศ หรือแนวทางปฏิบัติภายในอื่น ๆ ที่องค์กรกำหนดไว้ โดยมีผลครอบคลุมถึงระบบและบริการทางดิจิทัลทุกประเภทที่องค์กรนำมาใช้ในการดำเนินธุรกิจ

3. คำจำกัดความ (Definitions)

เพื่อให้การปฏิบัติตามนโยบายการกำกับดูแลและบริหารจัดการเทคโนโลยีสารสนเทศฉบับนี้เป็นไปอย่างชัดเจน เป็นมาตรฐานเดียวกัน และสามารถสื่อสารได้อย่างมีประสิทธิภาพระหว่างบุคลากรทุกระดับในองค์กร จึงกำหนดคำจำกัดความของคำศัพท์ที่เกี่ยวข้อง ดังต่อไปนี้

คำศัพท์	ความหมาย
1. บริษัท	บริษัท กรุงเทพดุสิตเวชการ จำกัด (มหาชน)
2. บริษัทย่อย	บริษัทที่บริษัท กรุงเทพดุสิตเวชการ จำกัด (มหาชน) มีอำนาจควบคุมการดำเนินงาน
3. องค์กร	บริษัท กรุงเทพดุสิตเวชการ จำกัด (มหาชน) และบริษัทย่อย
4. เทคโนโลยีสารสนเทศ (Information Technology)	ระบบ เทคโนโลยี หรือบริการที่เกี่ยวข้องกับการจัดเก็บ ประมวลผล รับ ส่ง หรือควบคุมข้อมูลและสารสนเทศในรูปแบบอิเล็กทรอนิกส์ ซึ่งครอบคลุมถึงข้อมูลหรือสารสนเทศ (data/information) อุปกรณ์คอมพิวเตอร์ (Hardware) ระบบปฏิบัติการ (Operating System) ระบบหรือโปรแกรมคอมพิวเตอร์ (Software) ระบบฐานข้อมูล (Database System) และระบบเครือข่ายสื่อสาร (Communication System) เป็นต้น
5. เทคโนโลยีดิจิทัล (Digital Technology)	เทคโนโลยีที่ใช้ข้อมูลในรูปแบบดิจิทัลเพื่อเพิ่มประสิทธิภาพในการดำเนินงานและการให้บริการ เช่น ระบบคลาวด์ (Cloud System) ปัญญาประดิษฐ์ (AI) การวิเคราะห์ข้อมูลขนาดใหญ่ (Big Data) บล็อกเชน (Blockchain)และแพลตฟอร์มออนไลน์
6. ปัญญาประดิษฐ์ (Artificial Intelligence: AI)	เทคโนโลยีหรือระบบที่สามารถเลียนแบบพฤติกรรมการเรียนรู้ วิเคราะห์ หรือการตัดสินใจของมนุษย์ โดยอาศัยอัลกอริทึมหรือแบบจำลองข้อมูล

คำศัพท์	ความหมาย
7. การกำกับดูแลเทคโนโลยีสารสนเทศ (IT Governance)	กระบวนการและโครงสร้างที่องค์กรใช้เพื่อกำหนดนโยบาย ทิศทาง และการกำกับดูแลการใช้เทคโนโลยีสารสนเทศให้สอดคล้องกับเป้าหมาย กลยุทธ์ และความเสี่ยงขององค์กร
8. ความมั่นคงปลอดภัยสารสนเทศ (Information Security)	มาตรการในการป้องกันข้อมูลและระบบเทคโนโลยีจากการเข้าถึง ใช้งาน เปิดเผย เปลี่ยนแปลง หรือทำลายโดยไม่ได้รับอนุญาต โดยยึดถือหลักสำคัญด้านความมั่นคงปลอดภัยของสารสนเทศ 3 ประการ ได้แก่ ความลับ (Confidentiality) ความถูกต้องครบถ้วน (Integrity) และความพร้อมใช้งาน (Availability)
9. ข้อมูลส่วนบุคคล (Personal Data)	ข้อมูลที่สามารถระบุถึงตัวบุคคลได้ ไม่ว่าจะทางตรงหรือทางอ้อม ตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562
10. ข้อมูลสุขภาพ (Health Information)	ข้อมูลที่เกี่ยวข้องกับสุขภาพ สถานะทางการแพทย์ การรักษาพยาบาล หรือข้อมูลทางชีวภาพของบุคคล ซึ่งถือเป็นข้อมูลอ่อนไหวตามกฎหมาย
11. การบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศ (IT Risk Management)	กระบวนการในการระบุ ประเมิน ควบคุม และติดตามความเสี่ยงที่เกี่ยวข้องกับการใช้เทคโนโลยีสารสนเทศ เพื่อจำกัดความเสียหายให้อยู่ในระดับที่องค์กรยอมรับได้

4. กรอบการดำเนินงานของการกำกับดูแลที่ดีด้านเทคโนโลยีสารสนเทศ (IT Governance)

การกำกับดูแลเทคโนโลยีสารสนเทศ (IT Governance) เป็นกระบวนการสำคัญในการสร้างความมั่นใจว่า การใช้เทคโนโลยีสารสนเทศขององค์กรนั้นมีประสิทธิภาพ โปร่งใส และสอดคล้องกับวัตถุประสงค์เชิงกลยุทธ์ขององค์กร โดยกรอบการดำเนินงานที่ดีควรครอบคลุมองค์ประกอบหลัก 5 ด้านตามแนวทางของ IT Governance Institute (ITGI) ดังต่อไปนี้

ภาพที่ 1. กรอบการดำเนินงานของการกำกับดูแลที่ดีด้านเทคโนโลยีสารสนเทศ

4.1 **การวางแนวทางเชิงกลยุทธ์** (Strategic Alignment)

องค์กรต้องจัดให้มีกระบวนการและกลไกในการวางแนวทางเชิงกลยุทธ์ด้านเทคโนโลยีสารสนเทศ และดิจิทัลให้สอดคล้องกับกลยุทธ์หลักขององค์กร เพื่อสนับสนุนการบรรลุเป้าหมายเชิงธุรกิจและสร้างความได้เปรียบในการแข่งขัน โดยมีแนวทางที่สำคัญ ดังนี้

- กำหนดให้กลยุทธ์ด้านเทคโนโลยีสารสนเทศและดิจิทัลมีความเชื่อมโยงกับแผนกลยุทธ์ขององค์กรในทุกระดับ ทั้งระยะสั้นและระยะยาว
- ส่งเสริมการมีส่วนร่วมและการประสานงานระหว่างฝ่ายเทคโนโลยีสารสนเทศกับหน่วยงานธุรกิจ เพื่อให้การพัฒนา การเลือกใช้ และการลงทุนด้านเทคโนโลยีเป็นไปในทิศทางเดียวกัน
- จัดให้มีกระบวนการวางแผน การประเมินความสำคัญ และการจัดลำดับความเร่งด่วนของโครงการหรือแผนงานด้านเทคโนโลยีสารสนเทศและดิจิทัลให้สอดคล้องกับลำดับความสำคัญของเป้าหมายองค์กร
- สนับสนุนการจัดสรรทรัพยากรอย่างมีประสิทธิภาพ โดยอิงจากข้อมูลเชิงกลยุทธ์และการตัดสินใจร่วมกันระหว่างผู้บริหารสายงานด้านเทคโนโลยีสารสนเทศและดิจิทัลและผู้บริหารสายงานด้านธุรกิจ

4.2 **การส่งมอบคุณค่า** (Value Delivery)

องค์กรต้องมีแนวทางและกลไกที่ชัดเจนในการส่งมอบคุณค่าจากการลงทุนด้านเทคโนโลยีสารสนเทศและดิจิทัล เพื่อให้มั่นใจว่าโครงการและบริการด้านเทคโนโลยีสารสนเทศ สามารถสร้างผลตอบแทนที่วัดผลได้ และตอบสนองต่อเป้าหมายเชิงกลยุทธ์ขององค์กร โดยมีแนวทางที่สำคัญ ดังนี้

- ตรวจสอบและประเมินให้แน่ใจว่าการลงทุนด้านเทคโนโลยีสารสนเทศสามารถสร้างผลตอบแทน (Return on Investment – ROI) และคุณค่าที่สามารถวัดผลได้อย่างชัดเจน
- มุ่งเน้นกระบวนการบริหารผลประโยชน์ (Benefits Realization) ตั้งแต่การวางแผน การกำหนดตัวชี้วัด จนถึงการติดตามผลการดำเนินงาน
- จัดให้มีการใช้ทรัพยากรด้านเทคโนโลยีสารสนเทศอย่างมีประสิทธิภาพสูงสุด ทั้งในด้านต้นทุน เวลา บุคลากร และเทคโนโลยี เพื่อสนับสนุนการดำเนินงานขององค์กร
- จัดให้มีระบบติดตามและประเมินความคืบหน้าโครงการด้านเทคโนโลยีสารสนเทศและดิจิทัลอย่างเป็นระบบ โดยใช้เกณฑ์ที่โปร่งใสและสามารถตรวจสอบได้ เพื่อให้การส่งมอบผลลัพธ์ตรงตามเป้าหมายที่กำหนดไว้

4.3 **การบริหารจัดการทรัพยากร** (Resource Management)

การบริหารจัดการทรัพยากรเทคโนโลยีสารสนเทศเป็นองค์ประกอบสำคัญของการกำกับดูแลเทคโนโลยีสารสนเทศที่ช่วยให้องค์กรสามารถใช้ทรัพยากรที่มีอยู่อย่างคุ้มค่าและเกิดประสิทธิภาพสูงสุด ทั้งนี้รวมถึงการวางแผน การจัดสรร และการพัฒนาอย่างยั่งยืน โดยมีแนวทางสำคัญ ดังนี้

- ครอบคลุมการบริหารจัดการทรัพยากรด้านเทคโนโลยีสารสนเทศ ได้แก่ บุคลากร งบประมาณ ระบบ โครงสร้างพื้นฐาน และข้อมูล ให้สามารถสนับสนุนภารกิจขององค์กรได้อย่างต่อเนื่องและยืดหยุ่น
- วางแผนและติดตามความสามารถในการรองรับภารกิจในระยะสั้นและระยะยาว (Capacity Planning) เพื่อลดความเสี่ยงจากการขาดแคลนหรือการใช้ทรัพยากรเกินความจำเป็น

- สนับสนุนการพัฒนาและเพิ่มพูนทักษะ ความรู้ และความสามารถของบุคลากรที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศเพื่อรองรับการเปลี่ยนแปลงทางเทคโนโลยีและความต้องการขององค์กร
- ส่งเสริมการบริหารจัดการโครงสร้างพื้นฐานด้านเทคโนโลยีสารสนเทศและดิจิทัลอย่างมีประสิทธิภาพ โดยคำนึงถึงความพร้อมใช้งาน ความมั่นคงปลอดภัย และความสามารถในการขยายตัวตามความต้องการทางธุรกิจ

4.4 **การบริหารความเสี่ยง** (Risk Management)

การบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศเป็นองค์ประกอบสำคัญของการกำกับดูแลเทคโนโลยีสารสนเทศที่ช่วยให้องค์กรสามารถตัดสินใจและดำเนินการเชิงรุกเพื่อลดผลกระทบจากความเสี่ยงที่อาจเกิดขึ้น พร้อมทั้งส่งเสริมความมั่นคงปลอดภัยและความต่อเนื่องของการดำเนินงาน โดยมีแนวทางสำคัญ ดังนี้

- ระบุ ประเมิน และจัดลำดับความสำคัญของความเสี่ยงที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศอย่างเป็นระบบ เช่น ความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ ความเสี่ยงด้านความเชื่อถือได้ของระบบ และความเสี่ยงจากการไม่ปฏิบัติตามกฎหมาย กฎระเบียบ หรือข้อกำหนดของหน่วยงานกำกับดูแล
- วางแผนและดำเนินมาตรการควบคุมภายในที่เหมาะสม เพื่อลดโอกาสเกิดความเสี่ยง และลดผลกระทบที่อาจเกิดขึ้นต่อองค์กร
- ส่งเสริมความพร้อมในการรับมือกับเหตุการณ์ผิดปกติ (Incident Response) และความสามารถในการรักษาความต่อเนื่องทางธุรกิจ (Business Continuity) รวมถึงการฟื้นฟูระบบและบริการที่สำคัญภายหลังเกิดเหตุ
- บูรณาการการบริหารความเสี่ยงเข้ากับกระบวนการตัดสินใจเชิงกลยุทธ์ขององค์กร เพื่อเสริมสร้างความมั่นคงปลอดภัยและความยั่งยืนในการใช้เทคโนโลยีสารสนเทศ

4.5 **การวัดและติดตามผลการดำเนินงาน** (Performance Measurement)

การวัดผลและติดตามประสิทธิภาพของการดำเนินงานด้านเทคโนโลยีสารสนเทศเป็นองค์ประกอบสำคัญในการกำกับดูแลเทคโนโลยีสารสนเทศและดิจิทัลที่มีประสิทธิภาพ เพื่อให้สามารถประเมินความคุ้มค่า ความสอดคล้องกับเป้าหมายองค์กร และผลลัพธ์ของการดำเนินงานในแต่ละด้านอย่างเป็นระบบ โดยมีแนวทางที่สำคัญ ดังนี้

- พัฒนาและใช้ระบบตัวชี้วัดผลการดำเนินงาน (Key Performance Indicators: KPIs) และกรอบการประเมิน (Assessment Framework) สำหรับวัดประสิทธิภาพและประสิทธิผลของกระบวนการ ระบบ และบริการด้านเทคโนโลยีสารสนเทศ
- ดำเนินการติดตาม ตรวจสอบ และรายงานผลการดำเนินงานเป็นประจำ เพื่อสนับสนุนการปรับปรุงอย่างต่อเนื่อง (Continuous Improvement) และการตัดสินใจเชิงกลยุทธ์ที่มีข้อมูลรองรับ
- ส่งเสริมวัฒนธรรมองค์กรที่ขับเคลื่อนด้วยข้อมูล (Data-Driven Culture) โดยการใช้ผลการวัดและข้อมูลเชิงสถิติเป็นเครื่องมือในการพัฒนาองค์กรอย่างยั่งยืน
- เชื่อมโยงผลการวัดกับระบบบริหารจัดการความเสี่ยง การจัดสรรทรัพยากร และการวางแผนกลยุทธ์ เพื่อให้เกิดผลลัพธ์สูงสุดต่อองค์กร

5. แนวทางปฏิบัติในการกำกับดูแลและบริหารจัดการเทคโนโลยีสารสนเทศระดับองค์กร

นโยบายฉบับนี้จัดทำขึ้นโดยมีวัตถุประสงค์เพื่อกำหนดกรอบแนวปฏิบัติในการกำกับดูแลและบริหารจัดการเทคโนโลยีสารสนเทศขององค์กรในระดับที่เหมาะสม สอดคล้องกับหลักการบริหารจัดการและการกำกับดูแลเทคโนโลยีสารสนเทศตามกรอบมาตรฐานสากล COBIT 2019 (Control Objectives for Information and Related Technologies) ซึ่งให้แนวทางเชิงโครงสร้างสำหรับการจัดการทรัพยากรสารสนเทศอย่างมีประสิทธิภาพและสอดคล้องกับเป้าหมายทางธุรกิจขององค์กร

นอกจากนี้ นโยบายฉบับนี้ยังอ้างอิงถึงแนวทางด้านการจัดการความมั่นคงปลอดภัยสารสนเทศตามมาตรฐาน ISO/IEC 27001:2022 ซึ่งเป็นมาตรฐานระบบบริหารจัดการความมั่นคงสารสนเทศ (Information Security Management System: ISMS) และ ISO 27799:2016 ซึ่งเป็นแนวทางเฉพาะด้านความมั่นคงสารสนเทศในด้านสุขภาพ รวมถึงแนวปฏิบัติที่แนะนำใน NIST Cybersecurity Framework (CSF) สำหรับการบริหารความเสี่ยงด้านไซเบอร์

นโยบายฉบับนี้จึงถือเป็นกลไกสำคัญในการส่งเสริมการปกป้องและรักษาทรัพย์สินสารสนเทศขององค์กร ให้มีความมั่นคงปลอดภัย เชื่อถือได้ และสามารถสนับสนุนการดำเนินธุรกิจได้อย่างต่อเนื่อง ทั้งนี้การดำเนินงานตามนโยบายดังกล่าวยังช่วยเสริมสร้างความเชื่อมั่นให้กับผู้มีส่วนได้ส่วนเสีย และสนับสนุนให้องค์กรสามารถบรรลุเป้าหมายเชิงกลยุทธ์ได้อย่างยั่งยืน ภายใต้กรอบการกำกับดูแลที่สอดคล้องกับมาตรฐานและข้อกำหนดสากล โดยครอบคลุมแนวปฏิบัติหลักในด้านต่าง ๆ ดังนี้

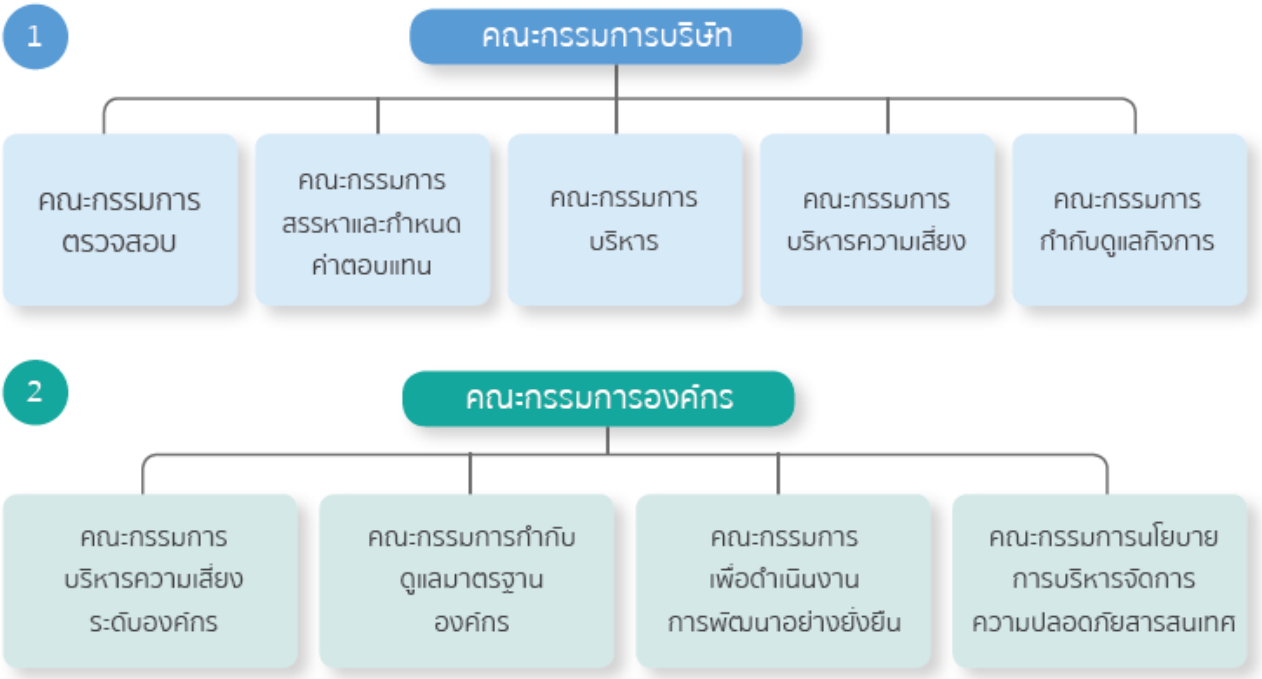
5.1 การกำกับดูแลและการบริหารจัดการเทคโนโลยีสารสนเทศ

บริษัทกำหนดให้การกำกับดูแลและการบริหารจัดการเทคโนโลยีสารสนเทศอยู่ภายใต้กรอบการกำกับดูแลกิจการที่ดี (Good Corporate Governance) โดยยึดถือหลักการสำคัญ อันได้แก่ ความโปร่งใส (Transparency) ความรับผิดชอบ (Accountability) การมีส่วนร่วม (Participation) ความสามารถในการตรวจสอบได้ (Auditability) และการปฏิบัติตามกฎหมาย กฎเกณฑ์และข้อกำหนดที่เกี่ยวข้อง (Compliance) เพื่อให้การดำเนินงานด้านเทคโนโลยีสารสนเทศขององค์กร เป็นไปอย่างมีประสิทธิภาพ มั่นคงปลอดภัย และสามารถสนับสนุนการบรรลุเป้าหมายเชิงกลยุทธ์ขององค์กรได้อย่างยั่งยืน

บริษัทได้บูรณาการการกำกับดูแลด้านเทคโนโลยีสารสนเทศและดิจิทัลเข้าไว้ในโครงสร้างการบริหารจัดการขององค์กรอย่างเป็นระบบ โดยมุ่งเน้นให้การกำหนดนโยบาย การบริหารความเสี่ยง การควบคุมภายใน และการติดตามประเมินผลเป็นไปในทิศทางเดียวกัน ภายใต้กรอบแนวทางและมาตรฐานสากลที่ได้รับการยอมรับ รวมถึงหลักเกณฑ์ตามประกาศสำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์ ว่าด้วยการกำกับดูแลและบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ

เพื่อเสริมสร้างกลไกการกำกับดูแลด้านเทคโนโลยีสารสนเทศให้มีความเข้มแข็งและมีประสิทธิภาพ บริษัทได้แต่งตั้งคณะกรรมการนโยบายการบริหารจัดการความปลอดภัยสารสนเทศ (Information Security Management Committee: ISMC) ซึ่งประกอบด้วยกรรมการบริษัทและผู้บริหารระดับสูงจากหน่วยงานที่เกี่ยวข้อง โดยคัดเลือกจากผู้มีคุณวุฒิ ความรู้ความสามารถ และประสบการณ์ที่เหมาะสม โดยเฉพาะอย่างยิ่งในด้านเทคโนโลยีสารสนเทศ ดิจิทัล และนวัตกรรม

คณะกรรมการนโยบายการบริหารจัดการความปลอดภัยสารสนเทศทำหน้าที่เป็นกลไกหลักในการกำกับดูแลด้านเทคโนโลยีสารสนเทศขององค์กร โดยมีบทบาทในการกำหนดนโยบาย วางแนวทางเชิงกลยุทธ์ พิจารณาและกลั่นกรองแผนงานโครงการ และการตัดสินใจที่มีนัยสำคัญ ตลอดจนติดตามและกำกับดูแลการดำเนินงานให้เป็นไปอย่างมีประสิทธิภาพ โปร่งใส สามารถตรวจสอบได้ และอยู่ภายใต้กรอบของหลักธรรมาภิบาล (Corporate Governance)



ภาพที่ 2. โครงสร้างการกำกับดูแลกิจการ

นอกจากนี้ คณะกรรมการนโยบายการบริหารจัดการความปลอดภัยสารสนเทศยังประสานความร่วมมือกับคณะกรรมการบริหารความเสี่ยงระดับองค์กร (Enterprise Risk Management Committee) และคณะกรรมการบริหารความเสี่ยง (Risk Management Committee) อย่างใกล้ชิด เพื่อบูรณาการการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศให้สอดคล้องกับกรอบการกำกับดูแลความเสี่ยงขององค์กรในภาพรวม โดยมุ่งเน้นให้การ ระบุ ประเมิน ควบคุม และติดตามความเสี่ยงที่เกี่ยวข้องกับระบบเทคโนโลยีสารสนเทศดำเนินไปอย่าง เป็นระบบ ครอบคลุม และมีประสิทธิภาพ เพื่อเสริมสร้างความมั่นใจว่าการดำเนินงานขององค์กรจะสามารถรองรับความเปลี่ยนแปลงและภัยคุกคามที่อาจเกิดขึ้นได้อย่างเหมาะสมและยั่งยืน

ทั้งนี้ คณะกรรมการตรวจสอบ ซึ่งดำรงสถานะเป็นคณะกรรมการอิสระ มีหน้าที่สอบทานความเพียงพอของการควบคุมภายใน การบริหารความเสี่ยง และการปฏิบัติตามกฎหมาย กฎเกณฑ์ และข้อกำหนดที่เกี่ยวข้องกับการดำเนินงานด้านเทคโนโลยีสารสนเทศ พร้อมทั้งเสนอข้อสังเกตและข้อเสนอแนะเชิงตรวจสอบต่อคณะกรรมการบริษัทโดยตรง

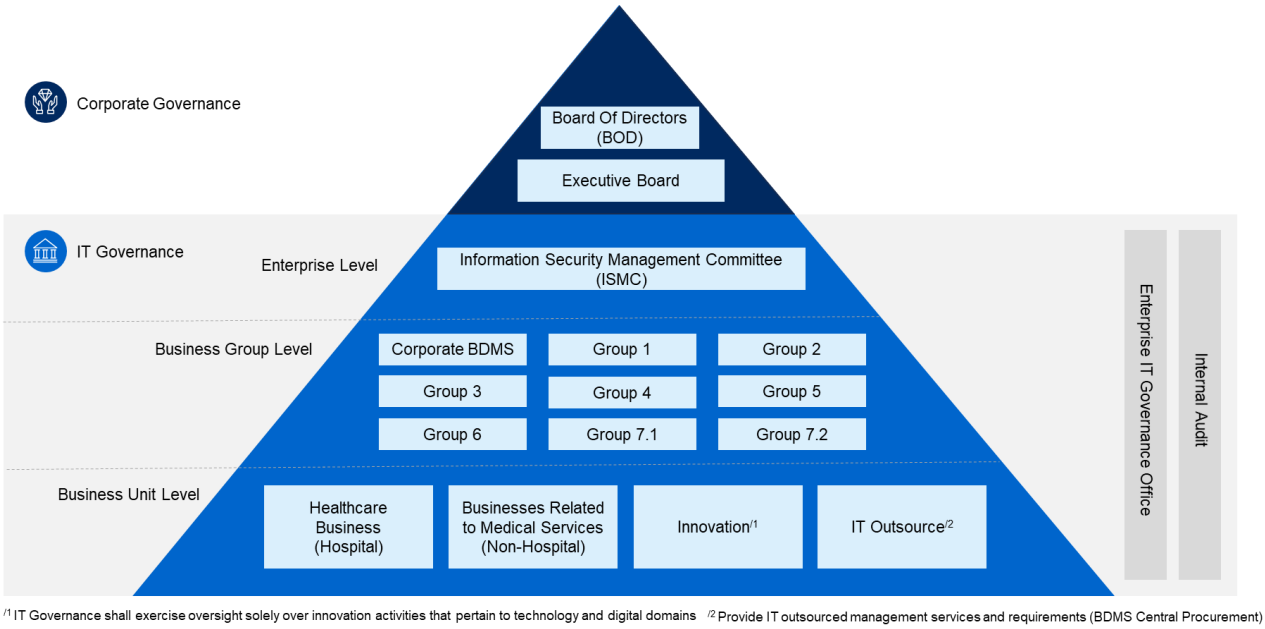
การบูรณาการการทำงานของคณะกรรมการองค์กรและคณะกรรมการบริษัท มีบทบาทสำคัญในการยกระดับระบบการกำกับดูแลด้านเทคโนโลยีสารสนเทศขององค์กร ให้มีความโปร่งใส มีความรับผิดชอบ และสามารถประเมินผลได้อย่างเป็นรูปธรรม สอดคล้องกับหลักธรรมาภิบาล และสนับสนุนเป้าหมายขององค์กรในการพัฒนาและเสริมสร้างศักยภาพด้านเทคโนโลยีสารสนเทศอย่างมั่นคง ปลอดภัย และยั่งยืนในระยะยาว

5.1.1 **โครงสร้างการกำกับดูแลเทคโนโลยีสารสนเทศ** (Governance Structure)

บริษัทได้กำหนดโครงสร้างการกำกับดูแลด้านเทคโนโลยีสารสนเทศให้ครอบคลุมทุกระดับขององค์กร เพื่อให้การดำเนินงานด้านเทคโนโลยีสารสนเทศ ความมั่นคงปลอดภัยทางไซเบอร์ ตลอดจนการประยุกต์ใช้เทคโนโลยีดิจิทัลและปัญญาประดิษฐ์ (Artificial Intelligence: AI) เป็นไปอย่างมีประสิทธิภาพ ปลอดภัย และสอดคล้องกับเป้าหมายเชิงกลยุทธ์ขององค์กรในระยะยาว

ทั้งนี้ บริษัทได้นำโครงสร้างการกำกับดูแลและบริหารจัดการด้านเทคโนโลยีสารสนเทศในรูปแบบ ผสมหรือสหพันธ์ (Hybrid / Federated Governance Model) มาใช้ โดยเป็นการผสานระหว่างแนวทางการกระจายอำนาจ (Decentralization) ไปยังกลุ่มธุรกิจและหน่วยธุรกิจ เพื่อเพิ่มความคล่องตัว ยืดหยุ่น และความเหมาะสมในการดำเนินงานตามบริบทเฉพาะของแต่ละกลุ่ม กับการดำรงไว้ซึ่งกลไกการควบคุมและกำกับดูแลจากส่วนกลาง (Centralized Oversight) เพื่อสร้างความสอดคล้องในระดับกลยุทธ์ การปฏิบัติตามข้อกำหนด และการใช้แนวทางปฏิบัติร่วมกันทั่วทั้งองค์กร โดยมีวัตถุประสงค์หลักเพื่อ

- ยกระดับประสิทธิภาพในการบริหารจัดการด้านเทคโนโลยีสารสนเทศ เพื่อให้การดำเนินงานด้านเทคโนโลยีมีความเป็นระบบ เชื่อมโยง และสามารถสนับสนุนภารกิจหลักขององค์กรได้อย่างมีประสิทธิภาพ
- เพิ่มคุณค่าเชิงกลยุทธ์จากการใช้เทคโนโลยีสนับสนุนธุรกิจ โดยใช้เทคโนโลยีเป็นกลไกสำคัญในการขับเคลื่อนนวัตกรรม การสร้างความได้เปรียบในการแข่งขัน และการสนับสนุนเป้าหมายเชิงกลยุทธ์ขององค์กร
- ลดความเสี่ยงเชิงระบบจากความซับซ้อนทางเทคโนโลยีผ่านกลไกการควบคุมภายใน การบริหารจัดการความเสี่ยง และการออกแบบระบบให้สามารถตรวจสอบและปรับปรุงได้อย่างต่อเนื่อง
- เสริมสร้างขีดความสามารถขององค์กรในการปรับตัวและเติบโตอย่างมั่นคง โดยสามารถรองรับการเปลี่ยนแปลงทางเทคโนโลยี ความคาดหวังของผู้มีส่วนได้ส่วนเสีย และพลวัตของเศรษฐกิจที่ขับเคลื่อนด้วยข้อมูลได้อย่างยืดหยุ่นและยั่งยืน



ภาพที่ 3. โครงสร้างการกำกับดูแลเทคโนโลยีสารสนเทศ (Governance Structure)

ภายใต้โครงสร้างการกำกับดูแลแบบผสมหรือแบบสหพันธ์ บริษัทได้กำหนดบทบาทและความรับผิดชอบอย่างชัดเจนในแต่ละระดับ ได้แก่ ระดับส่วนกลาง กลุ่มธุรกิจ และหน่วยธุรกิจ เพื่อให้การบริหารจัดการด้านเทคโนโลยี

สารสนเทศเป็นไปอย่างมีประสิทธิภาพ สอดคล้องกับกลยุทธ์องค์กร และสามารถตรวจสอบ ติดตาม และประเมินผลได้อย่างเป็นระบบและโปร่งใส

การจัดแบ่งบทบาทในลักษณะนี้มีเป้าหมายเพื่อสร้างสมดุลระหว่างการกำกับดูแลในระดับองค์กรกับการปฏิบัติงานในระดับปฏิบัติการ เพื่อให้สามารถตอบสนองต่อความต้องการทางธุรกิจ ความเสี่ยง และการเปลี่ยนแปลงของเทคโนโลยีได้อย่างคล่องตัว โดยมีรายละเอียดของแต่ละระดับ ดังนี้

1. **ระดับส่วนกลาง** (Enterprise / Corporate Level)

   ทำหน้าที่เป็นหน่วยงานกำกับดูแลหลักในระดับองค์กร โดยรับผิดชอบในการกำหนดนโยบายหลักด้านเทคโนโลยีสารสนเทศ มาตรฐานกลาง แนวทางปฏิบัติ และกรอบการประเมินผลการดำเนินงาน รวมถึงการกำหนดกลไกในการติดตาม ตรวจสอบ และให้ข้อเสนอแนะเชิงนโยบายแก่หน่วยงานในทุกระดับ เพื่อให้การดำเนินงานด้านเทคโนโลยีสารสนเทศเป็นไปอย่างมีธรรมาภิบาล สอดคล้องกับข้อกำหนด กฎหมาย และมาตรฐานที่เกี่ยวข้อง

2. **ระดับกลุ่มธุรกิจ** (Business Group Level)

   ทำหน้าที่ถ่ายทอดและประยุกต์ใช้นโยบายและมาตรฐานจากระดับส่วนกลางไปสู่การปฏิบัติจริงภายในกลุ่มธุรกิจ โดยคำนึงถึงลักษณะเฉพาะของการดำเนินงานในแต่ละกลุ่ม พร้อมทั้งรับผิดชอบในการกำกับดูแล ประเมิน และบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศในระดับกลุ่มธุรกิจ ให้สอดคล้องกับกรอบการบริหารความเสี่ยงในภาพรวมขององค์กร

3. **ระดับหน่วยธุรกิจ** (Business Unit Level)

   รับผิดชอบในการนำแนวนโยบาย มาตรฐาน และแนวปฏิบัติที่ได้รับมอบหมายไปปฏิบัติใช้ในระดับปฏิบัติการอย่างเคร่งครัด พร้อมทั้งดำเนินการจัดทำรายงานผลการดำเนินงาน การประเมินความเสี่ยง และการแจ้งเหตุการณ์ผิดปกติ (Incident Reporting) ต่อหน่วยงานที่เกี่ยวข้องอย่างต่อเนื่องและเป็นระบบ เพื่อให้สามารถตอบสนองต่อข้อกำหนดด้านความมั่นคงปลอดภัยสารสนเทศ และสนับสนุนการบรรลุเป้าหมายขององค์กรในทุกระดับ

5.1.2 กำหนดบทบาท หน้าที่ และความรับผิดชอบตามหลัก Three Lines of Defense

บริษัทจัดให้มีโครงสร้างการกำกับดูแลและบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศ ที่มีการถ่วงดุลอำนาจอย่างอิสระ (Check and Balance) และได้นำแนวทางการแบ่งระดับบทบาทและความรับผิดชอบในการบริหารจัดการและควบคุมความเสี่ยงตามหลัก "Three Lines of Defense" มาใช้ในการกำกับดูแลด้านเทคโนโลยีสารสนเทศ เทคโนโลยีดิจิทัล และความมั่นคงปลอดภัยทางไซเบอร์ เพื่อให้การดำเนินงานเป็นไปอย่างมีประสิทธิภาพ โปร่งใส และสามารถตรวจสอบได้ โดยมีการกำหนดบทบาท หน้าที่ และความรับผิดชอบออกเป็น 3 ระดับด้วยกัน คือ

1. **แนวป้องกันที่หนึ่ง** (First Line of Defense): **หน่วยงานปฏิบัติ**

เป็นแนวป้องกันด่านแรกขององค์กร โดยมีหน้าที่รับผิดชอบในการดำเนินงานตามนโยบาย มาตรฐาน และแนวทางที่องค์กรกำหนด ตลอดจนการบริหารจัดการความเสี่ยงภายในกระบวนการของตนเองอย่างมีประสิทธิภาพ

- ปฏิบัติงานตามนโยบาย มาตรฐาน และแนวปฏิบัติด้านเทคโนโลยีสารสนเทศ ความมั่นคงปลอดภัยไซเบอร์ และการคุ้มครองข้อมูลส่วนบุคคลที่องค์กรกำหนดไว้
- ระบุ ประเมิน และบริหารความเสี่ยงที่เกี่ยวข้องกับการดำเนินงานในระดับปฏิบัติการ
- ดำเนินมาตรการควบคุมภายในและจัดเก็บบันทึกหลักฐานที่เกี่ยวข้อง เพื่อรองรับการตรวจสอบและการสอบทานภายหลัง
- รายงานเหตุการณ์ผิดปกติ แนวโน้มความเสี่ยง หรือการละเมิดนโยบาย ต่อผู้บังคับบัญชาและหน่วยงานกำกับดูแลที่เกี่ยวข้องอย่างทันท่วงที
- สนับสนุนการสร้างวัฒนธรรมองค์กรที่ตระหนักรู้ด้านความมั่นคงปลอดภัยของระบบสารสนเทศและการใช้เทคโนโลยีอย่างมีความรับผิดชอบ

2. **แนวป้องกันที่สอง** (Second Line of Defense): **หน่วยงานกำกับและสนับสนุนการควบคุมความเสี่ยง**

ทำหน้าที่สนับสนุน กำกับ และติดตามการดำเนินงานของแนวป้องกันที่หนึ่ง โดยไม่ดำเนินงานเชิงปฏิบัติการโดยตรง แต่มีหน้าที่ในการพัฒนาแนวทาง กรอบการควบคุม และกำกับดูแลให้การบริหารความเสี่ยงเป็นไปตามนโยบาย กลยุทธ์ และมาตรฐานขององค์กร

- กำหนดแนวทางการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ ความมั่นคงปลอดภัยทางไซเบอร์ และการใช้เทคโนโลยีเกิดใหม่ให้สอดคล้องกับนโยบายขององค์กร กฎหมาย กฎระเบียบ และมาตรฐานที่เกี่ยวข้อง เพื่อรองรับการดำเนินงานในบริบทที่เปลี่ยนแปลงอย่างต่อเนื่อง
- สนับสนุนและให้คำปรึกษาแก่หน่วยงานที่เกี่ยวข้อง ในการ ออกแบบ ดำเนินการ และทบทวนมาตรการควบคุมภายใน ให้มีความเหมาะสม ครอบคลุมความเสี่ยงที่เกี่ยวข้อง และสามารถรองรับความซับซ้อนของกระบวนการทางธุรกิจและระบบเทคโนโลยีสารสนเทศได้อย่างมีประสิทธิภาพ
- ดำเนินการติดตาม ประเมิน และวิเคราะห์ความเสี่ยงเชิงระบบอย่างต่อเนื่อง พร้อมจัดทำรายงานเสนอผู้บริหารระดับสูงในกรณีที่พบความเสี่ยงที่เกินระดับความสามารถในการยอมรับขององค์กร (Risk Appetite) เพื่อสนับสนุนการตัดสินใจเชิงกลยุทธ์และการวางแผนมาตรการตอบสนองความเสี่ยงอย่างเหมาะสมและทันการณ์
- ตรวจสอบและประเมินความสอดคล้องของการดำเนินงานกับกฎหมาย ข้อบังคับ มาตรฐานสากล และนโยบายภายในองค์กร เพื่อให้มั่นใจว่ากิจกรรมด้านเทคโนโลยีสารสนเทศเป็นไปตามข้อกำหนดที่เกี่ยวข้องและลดความเสี่ยงด้านการไม่ปฏิบัติตาม (Non-compliance Risk)

3. **แนวป้องกันที่สาม** (Third Line of Defense): **หน่วยงานตรวจสอบภายใน**

ทำหน้าที่ในการให้บริการให้ความเชื่อมั่นอย่างเป็นอิสระและเที่ยงธรรม บนพื้นฐานของความเสี่ยง มุ่งเน้นการเพิ่มคุณค่าและการปรับปรุงการดำเนินงานของบริษัทให้ดีขึ้น โดยนำข้อกำหนดและวิธีการที่เป็นระบบ

มาใช้ในการประเมิน และปรับปรุงประสิทธิผลของการควบคุมภายใน การกำกับดูแลกิจการ และการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศขององค์กร

- ประเมินความเพียงพอและประสิทธิผลของการควบคุมภายในที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศ ความมั่นคงปลอดภัยไซเบอร์ และการใช้เทคโนโลยีเกิดใหม่
- ประเมินความสอดคล้องของการดำเนินงานกับนโยบายองค์กร มาตรฐานสากล และกฎหมาย/ข้อกำหนดที่เกี่ยวข้อง
- จัดทำรายงานผลการตรวจสอบ เพื่อนำเสนอข้อตรวจพบและข้อเสนอแนะในการปรับปรุงแก้ไข ต่อคณะกรรมการตรวจสอบ (Audit Committee) โดยตรง ติดตามการดำเนินการแก้ไขปรับปรุงตามข้อเสนอแนะการตรวจสอบ เพื่อให้มั่นใจว่ามีการตอบสนองและแก้ไขอย่างมีประสิทธิผล และสามารถลดความเสี่ยงได้อย่างยั่งยืน

5.1.3 **คณะกรรมการและหน่วยงานที่ทำหน้าที่กำกับดูและบริหารจัดการเทคโนโลยีสารสนเทศ**

บริษัทได้กำหนดให้มีการจัดตั้งคณะกรรมการและหน่วยงานเฉพาะทางที่มีบทบาทและหน้าที่โดยตรงในการกำกับดูแลและบริหารจัดการด้านเทคโนโลยีสารสนเทศ เพื่อให้การดำเนินงานในด้านดังกล่าวเป็นไปอย่างครอบคลุม เป็นระบบ มีประสิทธิภาพ และสามารถตรวจสอบได้ โดยยึดหลักการกำกับดูแลกิจการที่ดี (Good Governance) และสอดคล้องกับกรอบมาตรฐานสากล กฎหมาย และข้อกำหนดจากหน่วยงานกำกับดูแลที่เกี่ยวข้อง

การกำหนดบทบาทและความรับผิดชอบของคณะกรรมการและหน่วยงานที่เกี่ยวข้อง มีเป้าหมายเพื่อให้การใช้เทคโนโลยีสารสนเทศในองค์กรสามารถสนับสนุนกลยุทธ์ทางธุรกิจ การบริหารความเสี่ยง ความมั่นคงปลอดภัยไซเบอร์ การปกป้องข้อมูลส่วนบุคคล และการใช้เทคโนโลยีเกิดใหม่ ได้อย่างเหมาะสมและยั่งยืน โดยมีรายละเอียดของคณะกรรมการและหน่วยงานที่รับผิดชอบ ดังนี้

1. **คณะกรรมการนโยบายการบริหารจัดการความปลอดภัยสารสนเทศ** (Information Security Management Committee: ISMC)

   คณะกรรมการนโยบายการบริหารจัดการความปลอดภัยสารสนเทศ ทำหน้าที่เป็นหน่วยงานกำกับดูแลหลักในระดับองค์กร (Enterprise/Corporate Level) ในการกำกับดูแลและบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศให้สอดรับกับระดับความเสี่ยงที่ยอมรับได้ และเป็นส่วนหนึ่งของการบริหารความเสี่ยงขององค์กร (Enterprise Risk Management) โดยมีหน้าที่และความรับผิดชอบหลัก ดังนี้

   - กำหนดนโยบาย ทิศทาง และกรอบการกำกับดูแลด้านเทคโนโลยีสารสนเทศขององค์กร รวมถึงแผนงานด้านเทคโนโลยีสารสนเทศและดิจิทัล ให้มีความสอดคล้องกับเป้าหมายเชิงกลยุทธ์ขององค์กร โดยต้องสามารถรองรับการเปลี่ยนแปลงด้านเทคโนโลยีและการดำเนินธุรกิจในอนาคตได้อย่างเหมาะสม เพื่อเสริมสร้างขีดความสามารถในการแข่งขันและการเติบโตอย่างยั่งยืน
   - กำกับดูแลให้มีการจัดสรรทรัพยากรทางด้านเทคโนโลยีสารสนเทศให้มีความเพียงพอเหมาะสมและทรัพยากรบุคคลให้เพียงพอต่อการดำเนินธุรกิจ

- กำกับดูแลการกำหนดนโยบายเกี่ยวกับความเสี่ยงด้านเทคโนโลยีสารสนเทศเป็นลายลักษณ์อักษร โดยครอบคลุมถึงการจัดทำและอนุมัตินโยบายที่ชัดเจน พร้อมทั้งส่งเสริมและสนับสนุนให้มีการจัดทำแนวปฏิบัติ (Guidelines / Procedures) ที่สอดคล้องกับนโยบายดังกล่าว เพื่อใช้เป็นกรอบในการบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศขององค์กรอย่างมีประสิทธิภาพ และสอดคล้องกับกฎหมาย มาตรฐาน และข้อกำหนดที่เกี่ยวข้อง
- กำกับดูแลให้มีการสร้างความรู้และความตระหนักด้านความเสี่ยงด้านเทคโนโลยีสารสนเทศ แก่กรรมการ ผู้บริหาร และบุคลากรในองค์กรอย่างต่อเนื่องและมีประสิทธิผล
- กำกับดูแลให้มีการติดตาม ตรวจสอบ และรายงานผลการปฏิบัติตามนโยบาย ที่เกี่ยวข้องกับการกำกับดูแลความเสี่ยงด้านเทคโนโลยีสารสนเทศอย่างเป็นระบบ โดยต้องดำเนินการให้สอดคล้องกับกฎหมาย กฎระเบียบ มาตรฐานสากลที่เกี่ยวข้อง และข้อกำหนดจากหน่วยงานกำกับดูแล

2. **คณะกรรมการระดับกลุ่มธุรกิจ (กลุ่ม 1 – 7.2)**

   คณะกรรมการระดับกลุ่มธุรกิจ (Business Group Level) ทำหน้าที่ถ่ายทอดและประยุกต์ใช้นโยบาย มาตรฐาน และแนวทางปฏิบัติจากระดับส่วนกลางให้เหมาะสมกับบริบทของแต่ละกลุ่มธุรกิจ พร้อมทั้งบริหารจัดการการดำเนินงานให้สอดคล้องกับกลยุทธ์ ความเสี่ยง และเป้าหมายของกลุ่มธุรกิจ โดยมีหน้าที่และความรับผิดชอบหลัก ดังนี้

   - ถ่ายทอดและแปลงนโยบาย มาตรฐาน และแนวทางจากระดับส่วนกลาง ไปสู่การจัดทำแผนปฏิบัติการที่เหมาะสมกับบริบทของกลุ่มธุรกิจ และสามารถนำไปใช้ได้จริงในหน่วยธุรกิจภายใต้การกำกับ
   - กำกับดูแล ติดตาม และประเมินผลการดำเนินงานของหน่วยธุรกิจในกลุ่ม ให้เป็นไปตามกรอบนโยบายและมาตรฐานขององค์กร ตลอดจนสนับสนุนให้หน่วยธุรกิจสามารถปรับใช้แนวทางดังกล่าวได้อย่างมีประสิทธิภาพ
   - บริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศในระดับกลุ่ม รวมถึงจัดทำแผนตอบสนองต่อเหตุการณ์ผิดปกติ (Incident Response Plan) และแผนรองรับสถานการณ์ฉุกเฉินที่อาจเกิดขึ้น
   - ส่งเสริมและพัฒนาความรู้ ความเข้าใจ และความตระหนักในเรื่องเทคโนโลยี ความมั่นคงปลอดภัยไซเบอร์ และการประยุกต์ใช้ปัญญาประดิษฐ์ (AI) อย่างรับผิดชอบ ภายในกลุ่มธุรกิจ เพื่อยกระดับขีดความสามารถของหน่วยงานในกลุ่ม
   - จัดทำและสรุปผลการดำเนินงาน ความเสี่ยง และเหตุการณ์สำคัญในระดับกลุ่มธุรกิจอย่างสม่ำเสมอและเป็นระบบ เพื่อสนับสนุนการตัดสินใจเชิงกลยุทธ์ของผู้บริหารระดับสูงให้สามารถดำเนินการได้อย่างรอบด้านบนพื้นฐานของข้อมูลที่ถูกต้อง ครบถ้วนและทันเหตุการณ์ ตลอดจนเสริมสร้างความสามารถในการคาดการณ์ วางแผน และกำหนดมาตรการตอบสนองต่อความเสี่ยงหรือโอกาสที่อาจเกิดขึ้นได้อย่างมีประสิทธิภาพ

3. **คณะกรรมการระดับหน่วยธุรกิจ**

   คณะกรรมการระดับหน่วยธุรกิจ (Business Unit Level) ทำหน้าที่ในการดำเนินงานด้านเทคโนโลยีสารสนเทศในระดับปฏิบัติการ โดยยึดถือแนวนโยบาย มาตรฐาน และแนวทางปฏิบัติที่ได้รับมอบหมายจากระดับกลุ่มธุรกิจและระดับส่วนกลางอย่างเคร่งครัด โดยมีหน้าที่และความรับผิดชอบหลัก ดังนี้

- นำแนวนโยบาย มาตรฐาน และแนวทางด้านเทคโนโลยีสารสนเทศไปสู่การปฏิบัติจริงในกิจกรรมประจำวันและโครงการเฉพาะของหน่วยธุรกิจ ให้สอดคล้องกับเป้าหมายและข้อกำหนดขององค์กร
- บริหารจัดการระบบสารสนเทศ อุปกรณ์เทคโนโลยีสารสนเทศ และทรัพยากรที่เกี่ยวข้องภายในหน่วยงาน ให้มีประสิทธิภาพ ความมั่นคงปลอดภัย และความพร้อมใช้งานที่เหมาะสม
- ดำเนินการประเมินความเสี่ยง แจ้งเหตุการณ์ผิดปกติ และจัดทำรายงานผลการดำเนินงาน ส่งต่อไปยังหน่วยงานระดับกลุ่มธุรกิจหรือระดับส่วนกลางอย่างเป็นระบบและต่อเนื่อง
- ส่งเสริมการใช้งานเทคโนโลยีสารสนเทศอย่างมีความรับผิดชอบ ปลอดภัย และสอดคล้องกับข้อกำหนดด้านกฎหมาย มาตรฐาน และแนวปฏิบัติขององค์กร
- เสริมสร้างวัฒนธรรมองค์กรที่ให้ความสำคัญกับความมั่นคงปลอดภัยสารสนเทศ ความตระหนักรู้ด้านไซเบอร์ และการมีส่วนร่วมในการดำเนินงานด้านเทคโนโลยีในระดับปฏิบัติการ

4. **หน่วยงานธรรมาภิบาลด้านเทคโนโลยีสารสนเทศระดับองค์กร** (Enterprise IT Governance Office)
บริษัทได้จัดตั้งหน่วยงานธรรมาภิบาลด้านเทคโนโลยีสารสนเทศระดับองค์กร ทำหน้าที่เป็นกลไกระดับที่สองของโครงสร้างการควบคุม (Second Line of Defense) โดยมีบทบาทในการกำกับ ติดตาม และสนับสนุนการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ ดิจิทัล และปัญญาประดิษฐ์ (Artificial Intelligence: AI) ให้ดำเนินการได้อย่างมีประสิทธิภาพ สอดคล้องกับกรอบนโยบายขององค์กร และข้อกำหนดของหน่วยงานกำกับดูแล โดยมีหน้าที่และความรับผิดชอบหลัก ดังนี้
   - กำหนดกรอบการกำกับดูแลและบริหารจัดการเทคโนโลยีสารสนเทศและดิจิทัล (IT Governance Framework) รวมถึงนโยบาย มาตรฐานและแนวปฏิบัติที่เกี่ยวข้อง เพื่อให้การดำเนินงานด้านเทคโนโลยีขององค์กรมีทิศทางที่ชัดเจน โปร่งใส และสามารถตรวจสอบได้
   - กำหนดกรอบการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ (IT Risk Management Framework) รวมถึงการติดตามและประเมินประสิทธิผลของกระบวนการบริหารความเสี่ยงอย่างเป็นระบบ เพื่อให้สามารถระบุ ป้องกัน และจัดการกับความเสี่ยงที่อาจเกิดขึ้นได้อย่างเหมาะสม
   - ติดตามและประเมินผลการดำเนินงานด้านการกำกับดูแลและบริหารจัดการเทคโนโลยีสารสนเทศและดิจิทัล อย่างต่อเนื่อง พร้อมทั้งรายงานต่อคณะกรรมการนโยบายการบริหารจัดการความปลอดภัยสารสนเทศ และ/หรือ ผู้บริหารระดับสูงที่ได้รับมอบหมาย เพื่อใช้ประกอบการตัดสินใจและวางแผนเชิงกลยุทธ์
   - ส่งเสริมวัฒนธรรมองค์กรและสร้างความตระหนักรู้ ด้านการกำกับดูแลเทคโนโลยีสารสนเทศและดิจิทัล ให้เกิดขึ้นในทุกระดับขององค์กร โดยมุ่งเน้นให้บุคลากรมีความเข้าใจถึงบทบาทหน้าที่ ความรับผิดชอบ และสามารถมีส่วนร่วมในการดำเนินงานด้านเทคโนโลยีอย่างปลอดภัยและมีจริยธรรม
   - สนับสนุนการพัฒนาแนวทางการตรวจสอบและควบคุมภายในที่สอดคล้องกับการเปลี่ยนแปลงของเทคโนโลยี ความเสี่ยง และบริบททางธุรกิจ

5. **หน่วยงานตรวจสอบภายใน** (Internal Audit)
หน่วยงานตรวจสอบภายในมีบทบาทสำคัญในการประเมินความเพียงพอของการควบคุมภายใน การบริหารความเสี่ยง และการกำกับดูแลด้านเทคโนโลยีสารสนเทศขององค์กร โดยดำเนินการตรวจสอบอย่าง

เที่ยงธรรมและเป็นอิสระ โดยมีวัตถุประสงค์เพื่อให้การบริหารจัดการเทคโนโลยีสารสนเทศ ความมั่นคงปลอดภัยไซเบอร์ การปกป้องข้อมูล และการปฏิบัติตามข้อกำหนดกฎหมาย มีความโปร่งใส เป็นไปอย่างมีประสิทธิภาพและเป็นไปตามมาตรฐานที่องค์กรกำหนดไว้ โดยมีหน้าที่และความรับผิดชอบหลัก ดังนี้

- ประเมินความเพียงพอและประสิทธิผลของการควบคุมที่เกี่ยวข้องกับการดำเนินงานด้านเทคโนโลยีสารสนเทศ
- สอบทานการปฏิบัติตามนโยบาย แนวทางปฏิบัติ กฎหมาย และกฎเกณฑ์ของหน่วยงานกำกับดูแลที่เกี่ยวข้องกับการดำเนินงานด้านเทคโนโลยีสารสนเทศ
- ให้ข้อเสนอแนะการปรับปรุงกระบวนการทำงานและการควบคุมความเสี่ยงด้านเทคโนโลยีสารสนเทศเพื่อเสริมสร้างความโปร่งใสและความสามารถในการตรวจสอบได้
- จัดทำรายงานผลการตรวจสอบ เพื่อนำเสนอข้อตรวจพบและข้อเสนอแนะในการปรับปรุงแก้ไข ต่อคณะกรรมการตรวจสอบ (Audit Committee) โดยตรง

5.2 การบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ (IT Risk Management)

บริษัทตระหนักถึงความสำคัญของการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ และการรักษาความมั่นคงปลอดภัยของสารสนเทศ ในฐานะที่เป็นองค์ประกอบสำคัญของระบบการบริหารความเสี่ยงระดับองค์กร (Enterprise Risk Management: ERM) ซึ่งมีบทบาทในการสนับสนุนความสามารถขององค์กรในการรับมือกับความไม่แน่นอน ป้องกันผลกระทบจากเหตุการณ์ที่ไม่พึงประสงค์ และรักษาเสถียรภาพในการดำเนินงานอย่างต่อเนื่อง

เพื่อให้การบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศเป็นไปอย่างมีระบบและสามารถตรวจสอบได้ บริษัทจึงกำหนดให้มีการจัดทำนโยบายการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศอย่างเป็นลายลักษณ์อักษร เพื่อใช้เป็นกรอบแนวทางในการดำเนินการ ดังต่อไปนี้

5.2.1 บทบาทและความรับผิดชอบในการบริหารความเสี่ยง (Risk Ownership & Accountability)

องค์กรต้องกำหนด บทบาทหน้าที่ของผู้ที่เกี่ยวข้องในการบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศอย่างชัดเจน โดยรวมถึง

- คณะกรรมการบริหารความเสี่ยง (Risk Management Committee)
- คณะกรรมการบริหารความเสี่ยงระดับองค์กร (Enterprise Risk Management Committee)
- คณะกรรมการนโยบายการบริหารจัดการความปลอดภัยสารสนเทศ (Information Security Management Committee)
- ผู้บริหารระดับสูง (Executive Management)
- หน่วยงานกำกับดูแลความเสี่ยง
- หน่วยงานเทคโนโลยีสารสนเทศและหน่วยงานตรวจสอบภายใน

มีการกำหนดผู้รับผิดชอบหลัก (Risk Owner) สำหรับแต่ละความเสี่ยงที่ระบุไว้ พร้อมอำนาจและทรัพยากรที่เหมาะสมในการจัดการ

5.2.2 กระบวนการบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศ (IT Risk Management Process)

องค์กรต้องกำหนดให้มีการบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศอย่างเป็นระบบ ดังนี้

1. การระบุความเสี่ยง (Risk Identification)

   การระบุความเสี่ยงถือเป็นขั้นตอนสำคัญในกระบวนการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ เพื่อให้สามารถรับรู้ภัยคุกคาม ช่องโหว่ และเหตุการณ์ที่อาจส่งผลกระทบต่อระบบ เทคโนโลยี ข้อมูล และกระบวนการได้อย่างครอบคลุมและเป็นระบบ ทั้งนี้ ข้อมูลเกี่ยวกับความเสี่ยงต้องได้รับการทบทวนและปรับปรุงอย่างสม่ำเสมอ เพื่อให้สอดคล้องกับการเปลี่ยนแปลงของบริบทองค์กร ภัยคุกคามใหม่ เทคโนโลยีที่เกิดขึ้น และข้อกำหนดจากหน่วยงานกำกับดูแลที่เกี่ยวข้อง

2. การวิเคราะห์และประเมินความเสี่ยง (Risk Analysis and Evaluation)

   ดำเนินการประเมินระดับความเสี่ยงโดยพิจารณาความน่าจะเป็น (Likelihood) และผลกระทบ (Impact) ที่มีต่อความลับ (Confidentiality) ความถูกต้องครบถ้วน (Integrity) และความพร้อมใช้งานของระบบและข้อมูล (Availability) เพื่อจัดลำดับความสำคัญในการบริหารจัดการความเสี่ยงได้อย่างเหมาะสม

3. การจัดการความเสี่ยง (Risk Treatment)

   ดำเนินการเลือกใช้มาตรการควบคุมที่เหมาะสม เช่น การลด ถ่ายโอน ยอมรับ หรือหลีกเลี่ยงความเสี่ยง เพื่อควบคุมระดับความเสี่ยงที่เหลืออยู่ (Residual Risk) ให้อยู่ในระดับที่องค์กรสามารถยอมรับได้

4. การติดตามและทบทวนความเสี่ยง (Monitoring & Review)

   ดำเนินการตรวจสอบและติดตามสถานะความเสี่ยงและประสิทธิภาพของมาตรการควบคุมอย่างสม่ำเสมอ เพื่อให้สามารถปรับปรุงหรือแก้ไขแนวทางการบริหารความเสี่ยงได้อย่างเหมาะสมและทันต่อสถานการณ์.

5.2.3 **การบูรณาการกับระบบบริหารความเสี่ยงระดับองค์กร** (Integration with ERM)

บริษัทกำหนดให้มีการบูรณาการการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศเข้ากับกระบวนการบริหารความเสี่ยงระดับองค์กร (Enterprise Risk Management) โดยมุ่งเน้นการผนวกรวมข้อมูลความเสี่ยงด้านเทคโนโลยีสารสนเทศ ทั้งในเชิงกลยุทธ์และเชิงปฏิบัติการ เข้าไว้ในภาพรวมของการบริหารความเสี่ยงขององค์กร เพื่อให้สามารถ

- สนับสนุนการตัดสินใจเชิงกลยุทธ์ของฝ่ายบริหารด้วยข้อมูลความเสี่ยงที่มีความครบถ้วนและทันสมัย
- จัดลำดับความสำคัญของโครงการ การลงทุน และทรัพยากรในลักษณะบูรณาการ โดยพิจารณาจากความเสี่ยงและโอกาสที่เกี่ยวข้องในระดับองค์กร
- เชื่อมโยงความเสี่ยงด้านเทคโนโลยีเข้ากับความเสี่ยงด้านธุรกิจ และผลกระทบต่อเป้าหมายขององค์กรในมุมมองแบบองค์รวม

การบูรณาการนี้จะช่วยให้การบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศไม่ถูกดำเนินการแบบแยกส่วน (Silo) แต่สอดประสานกับโครงสร้างการบริหารองค์กรในทุกระดับ และส่งผลให้เกิดการบริหารความเสี่ยงที่มีประสิทธิภาพ ยั่งยืน และสามารถปรับตัวได้อย่างต่อเนื่องตามสภาพแวดล้อมที่เปลี่ยนแปลง

5.3 **การบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ** (Information Security Management)

บริษัทตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัยของสารสนเทศ โดยเฉพาะอย่างยิ่งการคุ้มครองข้อมูลที่มีลักษณะอ่อนไหว เช่น ข้อมูลส่วนบุคคล (Personal Data) และข้อมูลสุขภาพของผู้รับบริการ (Health Information) ซึ่งถือเป็นทรัพย์สินสารสนเทศที่มีความสำคัญยิ่งต่อความเชื่อมั่นและความน่าเชื่อถือขององค์กรในภาคธุรกิจบริการสุขภาพ

ในยุคที่เทคโนโลยีดิจิทัลและปัญญาประดิษฐ์ (Artificial Intelligence: AI) เข้ามามีบทบาทสำคัญในกระบวนการให้บริการทางการแพทย์ การวินิจฉัยโรค การวางแผนการรักษา และการบริหารจัดการภายในองค์กร บริษัทได้กำหนดแนวทางในการนำเทคโนโลยีดังกล่าวมาใช้อย่างมีความรับผิดชอบ ปลอดภัย และสอดคล้องกับหลักธรรมาภิบาลด้านข้อมูล โดยให้ความสำคัญกับการออกแบบระบบให้สามารถตรวจสอบได้ (Explainable AI) การประเมินผลกระทบด้านความมั่นคงปลอดภัยและความเป็นส่วนตัว (Security & Privacy Impact Assessment) ตลอดจนการกำหนดมาตรการควบคุมและแนวปฏิบัติในการใช้ข้อมูลที่อ่อนไหวอย่างเข้มงวด

เพื่อให้การบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศขององค์กรมีความครอบคลุม มีประสิทธิภาพ และสามารถรองรับภัยคุกคามทางไซเบอร์ที่มีความซับซ้อนและเปลี่ยนแปลงอย่างต่อเนื่อง บริษัทจึงได้กำหนดให้มีการจัดทำนโยบายการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ (Information Security Management Policy) เพื่อใช้เป็นกรอบแนวทางในการป้องกัน ควบคุม และตอบสนองต่อความเสี่ยงที่อาจส่งผลกระทบต่อระบบสารสนเทศ ทรัพยากรด้านเทคโนโลยีและข้อมูลสำคัญขององค์กร โดยยึดตามหลักการสำคัญของความมั่นคงปลอดภัยสารสนเทศ 3 ประการ ได้แก่

- ความลับของข้อมูล (Confidentiality) การป้องกันไม่ให้ข้อมูลที่สำคัญหรือข้อมูลส่วนบุคคลถูกเข้าถึงหรือเปิดเผยโดยไม่ได้รับอนุญาต
- ความถูกต้องครบถ้วนของข้อมูล (Integrity) การปกป้องข้อมูลและระบบให้คงอยู่ในสภาพที่ถูกต้อง ไม่ถูกดัดแปลง แก้ไข หรือลบโดยไม่ได้รับอนุญาต
- ความพร้อมใช้งานของระบบและข้อมูล (Availability) การรับประกันว่าระบบ ข้อมูล และบริการด้านเทคโนโลยีสารสนเทศขององค์กรสามารถเข้าถึงและใช้งานได้อย่างต่อเนื่อง โดยผู้ที่ได้รับอนุญาต

นโยบายฉบับนี้ถือเป็นส่วนหนึ่งของกรอบการทำงานด้านการกำกับดูแลกิจการที่ดีขององค์กร ซึ่งสะท้อนถึงความมุ่งมั่นของบริษัทในการบริหารจัดการเทคโนโลยีสารสนเทศอย่างมีประสิทธิภาพ โปร่งใส ตรวจสอบได้ โดยครอบคลุมประเด็นหลักที่สำคัญ ดังต่อไปนี้

5.3.1 มาตรการควบคุมด้านองค์กร (Organizational Controls)

5.3.1.1 โครงสร้างการบริหารงานเพื่อการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ (Organization of information technology security)

5.3.1.2 การบริหารจัดการนโยบายความมั่นคงสารสนเทศ (Policies for Information Security)

5.3.1.3 การบริหารจัดการทรัพย์สินด้านเทคโนโลยีสารสนเทศ (IT Asset Management)

5.3.1.4 การรักษาความมั่นคงปลอดภัยของข้อมูล (Information Security)

5.3.1.5 การควบคุมการเข้าถึงข้อมูลและระบบเทคโนโลยีสารสนเทศ (Access Control)

5.3.1.6 การบริหารจัดการเหตุการณ์ด้านความมั่นคงปลอดภัยสารสนเทศ (IT Security Incident Management)

5.3.1.7 การจัดการความต่อเนื่องทางธุรกิจ (Business Continuity Management)

5.3.1.8 การจัดการภัยคุกคามไซเบอร์ (Threat Intelligence Management)

5.3.1.9 การบริหารจัดการบุคคลภายนอก (IT Third-party Management)

5.3.2 มาตรการควบคุมด้านบุคลากร (People Controls)

5.3.2.1 การคัดกรองบุคลากรและจัดการสิทธิ์เข้าถึงข้อมูล (Personnel Screening and Access Management)

5.3.2.2 การจัดการความตระหนักรู้และฝึกอบรม (Awareness and Training)

5.3.3 มาตรการการควบคุมทางกายภาพ (Physical Controls)

5.3.3.1 การรักษาความมั่นคงปลอดภัยของพื้นที่ทางกายภาพ (Physical Security)

5.3.3.2 การจัดการอุปกรณ์และสิ่งแวดล้อมที่เกี่ยวข้องกับระบบสารสนเทศ (Equipment and Environment Security)

5.3.4 มาตรการควบคุมด้านเทคโนโลยี (Technological Controls)

5.3.4.1 การควบคุมการเข้ารหัสและปกป้องข้อมูล (Encryption and Data Protection)

5.3.4.2 การรักษาความปลอดภัยระบบเครือข่ายและการสื่อสารข้อมูล (Network and Communication Security)

5.3.4.3 การรักษาความมั่นคงปลอดภัยในการปฏิบัติงานด้านเทคโนโลยีสารสนเทศ (IT Operations Security)

5.3.4.4 การพัฒนาและบำรุงรักษาระบบสารสนเทศและ AI อย่างมั่นคงปลอดภัย (Secure Development and Maintenance)

5.3.4.5 การจัดการรหัสผ่านและการยืนยันตัวตน (Authentication and Identity Management)

ทั้งนี้ การปฏิบัติตามนโยบายดังกล่าวจะช่วยเสริมสร้างความเชื่อมั่นให้กับผู้มีส่วนได้ส่วนเสีย และรักษามาตรฐานความปลอดภัยขององค์กรให้เป็นไปตามกรอบกฎหมายและข้อกำหนดที่เกี่ยวข้อง

5.4 การปฏิบัติตามกฎหมายและกฎเกณฑ์ที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศ (IT Compliance)

บริษัทตระหนักถึงความสำคัญของการปฏิบัติตามกฎหมาย ระเบียบ และแนวปฏิบัติที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศ ซึ่งครอบคลุมประเด็นด้านความมั่นคงปลอดภัยของระบบสารสนเทศ การคุ้มครองข้อมูลส่วนบุคคล การรักษาความปลอดภัยทางไซเบอร์ การดำเนินธุรกรรมทางอิเล็กทรอนิกส์ ตลอดจนข้อกำหนดเฉพาะในอุตสาหกรรมสุขภาพ ทั้งนี้เพื่อป้องกันความเสี่ยงทางกฎหมาย เสริมสร้างความน่าเชื่อถือ และคงไว้ซึ่งความยั่งยืนขององค์กรในระยะยาว บริษัทจึงได้กำหนดแนวทางในการกำกับการปฏิบัติตามกฎเกณฑ์ที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศ ดังนี้

5.4.1 โครงสร้างองค์กร

องค์กรต้องกำหนดโครงสร้างที่ชัดเจนในการดำเนินงานด้านการกำกับดูแลการปฏิบัติตามกฎเกณฑ์ที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศ (IT Compliance) โดยครอบคลุมแนวทางสำคัญ ดังต่อไปนี้

1. องค์กรต้องจัดให้มีการดำเนินการด้านการกำกับดูแลการปฏิบัติตามกฎเกณฑ์ที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศ โดยสามารถดำเนินการได้หลายรูปแบบ เช่น
   - การจัดตั้งเป็นหน่วยงานเฉพาะด้าน IT Compliance
   - การรวมเป็นส่วนหนึ่งของหน่วยงานที่ดูแลการปฏิบัติตามกฎเกณฑ์ขององค์กร
   - หรือรูปแบบอื่นที่เหมาะสมกับโครงสร้างขององค์กร

ทั้งนี้ ต้องมั่นใจว่าโครงสร้างดังกล่าวมีความเป็นอิสระเพียงพอ สามารถดำเนินงานได้อย่างครบถ้วน มีประสิทธิภาพ และไม่ถูกแทรกแซงจากหน่วยงานผู้ปฏิบัติ (First Line of Defense)

2. ต้องกำหนดสายการรายงานของผู้รับผิดชอบด้าน IT Compliance ให้มีความเป็นอิสระจากสายงานที่เกี่ยวข้องกับการดำเนินงานประจำวัน โดยให้รายงานต่อหัวหน้าหน่วยงานด้านการกำกับดูแลการปฏิบัติตามกฎเกณฑ์ ซึ่งมีสายการรายงานตรงต่อคณะกรรมการที่เกี่ยวข้อง เช่น คณะกรรมการที่ทำหน้าที่กำกับดูแลบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ หรือคณะกรรมการที่ทำหน้าที่กำกับดูแลการปฏิบัติตามกฎเกณฑ์ เป็นต้น
3. ผู้รับผิดชอบงานด้านการกำกับดูแลการปฏิบัติตามกฎเกณฑ์ที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศ ต้องมีคุณสมบัติที่เหมาะสม ได้แก่
   - มีความรู้และความเข้าใจเกี่ยวกับกฎหมาย กฎระเบียบ และข้อกำหนดด้านเทคโนโลยีสารสนเทศ
   - มีประสบการณ์ด้านการกำกับดูแล หรือด้านเทคโนโลยีที่เกี่ยวข้อง
   - ได้รับการฝึกอบรมอย่างต่อเนื่องทั้งในด้านข้อกำหนดกฎเกณฑ์และความรู้ด้านเทคโนโลยีใหม่ ๆ เพื่อให้สามารถปรับตัวและปฏิบัติงานได้อย่างมีประสิทธิภาพและทันสมัย

5.4.2 การปฏิบัติงานด้านการกำกับการปฏิบัติตามกฎเกณฑ์ที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศ

องค์กรต้องกำหนดกระบวนการที่ชัดเจนและมีประสิทธิภาพในการกำกับดูแลการปฏิบัติตามกฎหมาย กฎระเบียบ มาตรฐาน และข้อกำหนดที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศ เพื่อป้องกันการฝ่าฝืนหรือการไม่ปฏิบัติตามข้อบังคับของหน่วยงานกำกับดูแล โดยอย่างน้อยต้องครอบคลุมองค์ประกอบสำคัญ ดังต่อไปนี้

1. ต้องดำเนินการระบุและประเมินความเสี่ยงที่เกี่ยวข้องกับกฎหมายและกฎเกณฑ์ด้านเทคโนโลยีสารสนเทศอย่างครอบคลุม เช่น กฎหมายว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ กฎหมายว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ กฎหมายว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ และกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล (PDPA) เพื่อใช้เป็นพื้นฐานในการวางมาตรการป้องกันการละเมิด หรือการไม่ปฏิบัติตามข้อกำหนด
2. ต้องจัดทำแผนการบริหารความเสี่ยงด้านการปฏิบัติตามกฎหมายและกฎเกณฑ์ด้านเทคโนโลยีสารสนเทศประจำปี โดยให้สอดคล้องกับระดับความเสี่ยงที่ได้จากการประเมิน และครอบคลุมการดำเนินการ เช่น
   - การสอบทานระเบียบ ข้อบังคับ และนโยบายที่พนักงานต้องถือปฏิบัติ
   - การตรวจสอบการปฏิบัติตามกฎเกณฑ์ที่มีผลบังคับใช้
   - การเผยแพร่ความรู้และจัดฝึกอบรมให้แก่บุคลากรในเรื่องกฎหมายและข้อกำหนดที่เกี่ยวข้อง
3. ต้องมีกระบวนการหรือระบบการติดตาม ตรวจสอบ และรายงานผลการสอบทานการปฏิบัติตามกฎเกณฑ์อย่างสม่ำเสมอ โดยให้รวมถึง
   - การสรุปเหตุการณ์ที่พบว่ามีการไม่ปฏิบัติตามข้อกำหนด
   - มาตรการแก้ไขและข้อเสนอแนะที่ได้รับจากการสอบทาน
   - รายงานผลการดำเนินการตามข้อเสนอแนะดังกล่าวต่อคณะกรรมการที่ได้รับมอบหมาย หรือผู้บริหารระดับสูงตามที่องค์กรกำหนด

5.5 การตรวจสอบด้านเทคโนโลยีสารสนเทศ (IT Audit)

บริษัทกำหนดให้มีการตรวจสอบด้านเทคโนโลยีสารสนเทศอย่างเป็นระบบ บนพื้นฐานของความเสี่ยง ทั้งนี้ การตรวจสอบต้องดำเนินการโดยผู้ตรวจสอบที่มีความเป็นอิสระ มีคุณสมบัติ และความเชี่ยวชาญเพียงพอ เพื่อให้สามารถประเมินความเหมาะสมและประสิทธิผลของมาตรการควบคุมภายในได้อย่างรอบด้าน การตรวจสอบดังกล่าวครอบคลุมถึงการประเมินการควบคุมภายใน การบริหารความเสี่ยง การปฏิบัติตามกฎหมาย กฎระเบียบ และข้อกำหนดที่เกี่ยวข้อง เพื่อให้มั่นใจว่าระบบงานมีความถูกต้อง เชื่อถือได้ และมีการเก็บรักษาข้อมูลอย่างปลอดภัย รวมถึงมีความพร้อมใช้งานหากเกิดภัยคุกคาม

องค์กรต้องจัดให้มีการติดตามและกำกับดูแลการดำเนินการแก้ไขประเด็นที่ได้จากการตรวจสอบให้แล้วเสร็จภายในระยะเวลาที่กำหนด พร้อมทั้งนำผลการตรวจสอบไปใช้ในการพัฒนาและปรับปรุงการบริหารจัดการเทคโนโลยีสารสนเทศอย่างต่อเนื่อง โดยยึดหลักการของวงจรการปรับปรุงคุณภาพ (Plan–Do–Check–Act: PDCA) เพื่อยกระดับประสิทธิภาพในการควบคุมและกำกับดูแลเทคโนโลยีสารสนเทศขององค์กรให้สอดคล้องกับมาตรฐานสากลและความคาดหวังของผู้มีส่วนได้ส่วนเสีย

5.5.1 โครงสร้างองค์กร

1. องค์กรต้องจัดให้มีการดำเนินการในงานตรวจสอบด้านเทคโนโลยีสารสนเทศ (IT audit function) โดยสามารถจัดตั้งเป็นหน่วยงานที่รับผิดชอบการตรวจสอบด้านเทคโนโลยีสารสนเทศ หรืออยู่ภายใต้หน่วยงานตรวจสอบภายใน ทั้งนี้ ผู้ตรวจสอบต้องดำรงความเป็นอิสระ และปฏิบัติตามหลักจริยธรรมวิชาชีพตรวจสอบภายใน เพื่อให้ผลการตรวจสอบมีความน่าเชื่อถือ โปร่งใส และสามารถนำไปใช้ในการปรับปรุงกระบวนการควบคุมและบริหารจัดการเทคโนโลยีสารสนเทศขององค์กรอย่างมีประสิทธิภาพ
2. กำหนดสายการรายงานที่เป็นอิสระ โดยหัวหน้าหน่วยงานตรวจสอบภายในมีสายบังคับบัญชาขึ้นตรงต่อคณะกรรมการตรวจสอบ (Audit Committee)
3. ผู้รับผิดชอบงานด้านการตรวจสอบเทคโนโลยีสารสนเทศต้องมีความรู้ ประสบการณ์และความเชี่ยวชาญเกี่ยวกับการตรวจสอบด้านเทคโนโลยีสารสนเทศ ซึ่งอาจเป็นผู้ตรวจสอบภายในหรือผู้ตรวจสอบภายนอก ที่มีความเป็นอิสระจากหน่วยงานที่ทำหน้าที่ปฏิบัติงานด้านเทคโนโลยีสารสนเทศและหน่วยงานที่ทำหน้าที่บริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศและกำกับดูแลการปฏิบัติตามกฎเกณฑ์ที่เกี่ยวข้องกับการดำเนินงานด้านเทคโนโลยีสารสนเทศ โดยผู้ตรวจสอบดังกล่าวต้องผ่านการรับรองหรือมีวุฒิบัตรตามข้อกำหนดของสำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์ (ก.ล.ต.) หรือหน่วยงานที่เกี่ยวข้อง
4. ผู้ตรวจสอบด้านเทคโนโลยีสารสนเทศต้องได้รับการฝึกอบรม เพิ่มความรู้ด้านเทคโนโลยีสารสนเทศและเทคโนโลยีใหม่อย่างต่อเนื่อง เพื่อให้ผู้ตรวจสอบสามารถนำมาปรับใช้กับวิธีการตรวจสอบได้ทันกับแนวโน้มและการพัฒนาทางด้านเทคโนโลยีสารสนเทศ

5.5.2 การปฏิบัติงานด้านการตรวจสอบเทคโนโลยีสารสนเทศ

บริษัทกำหนดให้มีการดำเนินการตรวจสอบด้านเทคโนโลยีสารสนเทศอย่างน้อยปีละหนึ่งครั้ง ตามแผนการตรวจสอบที่ได้รับการอนุมัติจากคณะกรรมการตรวจสอบ (Audit Committee) โดยมีกระบวนการอย่างน้อยครอบคลุม ดังนี้

1. **การกำหนดแผนและขอบเขตการตรวจสอบ** (IT Audit Plan)
    - หน่วยงานตรวจสอบภายในต้องจัดทำแผนการตรวจสอบด้านเทคโนโลยีสารสนเทศตามแนวทางการประเมินความเสี่ยง (Risk Based Audit Plan) โดยกำหนดขอบเขตให้ครอบคลุมการปฏิบัติงาน และระบบงานที่เกี่ยวข้องด้านเทคโนโลยีสารสนเทศอย่างรอบด้าน
    - การจัดทำแผนการตรวจสอบต้องอาศัยการรวบรวมข้อมูลต่าง ๆ เพื่อศึกษาและทำความเข้าใจเกี่ยวกับองค์กร เช่น โครงสร้างการบริหารจัดการ กระบวนการปฏิบัติงาน ระบบงานด้านเทคโนโลยีสารสนเทศ ผลการประเมินความเสี่ยงขององค์กร (Corporate Risk Profile) ความเห็นของผู้บริหารระดับสูง ตลอดจประสิทธิภาพและประสิทธิผลของการควบคุมภายใน เป็นต้น เพื่อนำมาประกอบการกำหนดขอบเขตของงานตรวจสอบทั้งหมด (Audit Universe) ที่ครอบคลุมทั่วทั้งองค์กร
    - หน่วยงานตรวจสอบภายในต้องดำเนินการประเมินความเสี่ยงในเชิงระบบและกระบวนการ เพื่อใช้เป็นพื้นฐานในการกำหนดลำดับความสำคัญและกำหนดแนวทางการตรวจสอบที่เหมาะสม
    - จัดทำแผนการตรวจสอบและนำเสนอคณะกรรมการตรวจสอบ (Audit Committee) เพื่อพิจารณาให้ความเห็นชอบ โดยหัวหน้าหน่วยงานตรวจสอบภายในมีหน้าที่ในการทบทวนและปรับปรุงแผนการตรวจสอบตามความจำเป็น หรือเมื่อมีการเปลี่ยนแปลงสาระสำคัญในแผนการตรวจสอบภายในประจำปี ทั้งนี้ ต้องนำเสนอคณะกรรมการตรวจสอบเพื่อพิจารณาอนุมัติแผนฉบับปรับปรุงอีกครั้ง
2. **การตรวจสอบ** (Audit Execution)
    - ผู้ตรวจสอบภายในต้องดำเนินการตรวจสอบอย่างเป็นระบบและสอดคล้องกับขั้นตอนที่กำหนดไว้ในแผนการตรวจสอบที่ได้รับความเห็นชอบจากคณะกรรมการตรวจสอบ (Audit Committee) ทั้งนี้ ต้องยึดถือมาตรฐานสากลว่าด้วยการปฏิบัติงานวิชาชีพตรวจสอบภายใน และจรรยาบรรณของผู้ตรวจสอบภายใน เป็นกรอบแนวทางในการปฏิบัติงาน เพื่อให้ได้มาซึ่งผลการตรวจสอบที่มีคุณภาพ เชื่อถือได้ และเป็นที่ยอมรับจากหน่วยงานต่าง ๆ ภายในองค์กร
    - กระบวนการตรวจสอบต้องมุ่งเน้นการรวบรวมข้อมูลและหลักฐานที่เพียงพอเหมาะสม เพื่อใช้ในการวิเคราะห์และแสดงความเห็นต่อการประเมินผลการดำเนินงาน และประสิทธิผลของการควบคุมด้านเทคโนโลยีสารสนเทศ ว่ามีความสอดคล้องกับวัตถุประสงค์ที่กำหนด รวมถึงมีการปฏิบัติตามมาตรฐาน แนวทาง และขั้นตอนที่องค์กร กำหนด ตลอดจนต้องสอดคล้องกับกฎหมาย กฎเกณฑ์ และข้อกำหนดที่เกี่ยวข้อง รวมถึงแนวปฏิบัติตามมาตรฐานสากลที่ได้รับการยอมรับอย่างกว้างขวาง
3. **การรายงานผลการตรวจสอบและติดตาม** (Audit Reporting and Follow-up)
    - หน่วยงานตรวจสอบภายในต้องกำหนดให้มีการสรุปผลการตรวจสอบ รวมถึงประเด็นที่ตรวจพบและข้อเสนอแนะในการปรับปรุงแก้ไข ให้แก่ผู้บริหารของหน่วยงานผู้รับการตรวจสอบโดยตรง เพื่อสร้างความเข้าใจร่วมกันในประเด็นที่ต้องดำเนินการแก้ไข และส่งเสริมให้เกิดการปรับปรุงแก้ไขอย่างมีประสิทธิภาพ
    - ผู้ตรวจสอบต้องจัดทำรายงานผลการตรวจสอบ (Audit Report) อย่างเป็นลายลักษณ์อักษร โดยต้องประกอบด้วยสาระสำคัญ ได้แก่ วัตถุประสงค์ ขอบเขต วิธีการตรวจสอบ ผลการตรวจสอบ ข้อเสนอแนะ

ในการปรับปรุงแก้ไขที่สามารถนำไปปฏิบัติได้จริง และความเห็นของหน่วยรับตรวจ ตลอดจนแนวทางการดำเนินงานของหน่วยงานที่เกี่ยวข้อง ทั้งนี้ รายงานต้องนำเสนอต่อคณะกรรมการตรวจสอบ (Audit Committee) เพื่อพิจารณา และนำส่งผู้บริหารระดับสูงที่เกี่ยวข้องต่อไป

- หน่วยงานตรวจสอบภายในต้องจัดให้มีการติดตามการแก้ไขประเด็นการตรวจสอบอย่างเป็นระบบ (Issue Tracking and Follow-up) เพื่อให้มั่นใจว่าหน่วยงานที่เกี่ยวข้องได้นำข้อเสนอแนะไปปฏิบัติอย่างมีประสิทธิผล หรือในกรณีที่ไม่สามารถดำเนินการได้ ให้มีการบันทึกการยอมรับความเสี่ยงโดยผู้บริหารระดับสูงอย่างชัดเจน และต้องรายงานผลการติดตามความคืบหน้าต่อคณะกรรมการตรวจสอบ (Audit Committee) เป็นระยะอย่างน้อยปีละหนึ่งครั้ง หรือบ่อยครั้งตามความเหมาะสมกับความเสี่ยงของประเด็นที่ตรวจพบ

5.6 การบริหารจัดการโครงการด้านเทคโนโลยีสารสนเทศ (IT Project Management)

บริษัทตระหนักถึงความสำคัญของการบริหารจัดการโครงการเทคโนโลยีสารสนเทศและดิจิทัลอย่างเป็นระบบ เพื่อให้การดำเนินโครงการเป็นไปอย่างมีประสิทธิภาพ โปร่งใส ตรวจสอบได้ และสามารถสร้างคุณค่าให้แก่องค์กรได้อย่างแท้จริง ทั้งนี้ บริษัทได้กำหนดแนวทางการบริหารจัดการโครงการที่ครอบคลุมตลอดวงจรชีวิตของโครงการ โดยเน้นการบูรณาการหลักการกำกับดูแล การบริหารความเสี่ยง และความมั่นคงปลอดภัยสารสนเทศอย่างเหมาะสม ดังนี้

5.6.1 การอนุมัติโครงการและการจัดลำดับความสำคัญ (Project Approval and Prioritization)

องค์กรต้องกำหนดให้โครงการที่เกี่ยวข้องกับการพัฒนา หรือปรับปรุงระบบเทคโนโลยีสารสนเทศและดิจิทัล ต้องผ่านกระบวนการพิจารณาและอนุมัติโดยคณะกรรมการที่ได้รับมอบหมายหรือคณะกรรมการที่มีอำนาจหน้าที่ตามที่กำหนดไว้ในนโยบายระดับองค์กร โดยพิจารณาจากปัจจัยสำคัญ ได้แก่ ความสอดคล้องกับวิสัยทัศน์และกลยุทธ์องค์กร มูลค่าเชิงธุรกิจ ระดับความเสี่ยง และความพร้อมของทรัพยากรที่เกี่ยวข้อง พร้อมทั้งจัดลำดับความสำคัญของโครงการเพื่อให้การใช้ทรัพยากรและงบประมาณอย่างมีประสิทธิภาพสูงสุด

5.6.2 การบริหารวงจรชีวิตของโครงการ (Project Lifecycle Management)

กำหนดกรอบการบริหารจัดการโครงการ (Project Management Framework) ที่ชัดเจนเป็นลายลักษณ์อักษร เพื่อใช้เป็นแนวทางบริหารจัดการโครงการตามวงจรชีวิตของโครงการ (Project Lifecycle) ที่ประกอบด้วยขั้นตอนหลัก ได้แก่ การริเริ่มโครงการ การวางแผน การดำเนินการ การตรวจสอบและควบคุม และการปิดโครงการ พร้อมทั้งส่งเสริมการใช้แนวทางที่เป็นมาตรฐาน เช่น PMBOK หรือ Agile/Hybrid ตามลักษณะของโครงการ

5.6.3 การประเมินผลกระทบด้านความเสี่ยงและแผนความต่อเนื่องทางธุรกิจ (Risk and BCP Assessment)

โครงการที่มีผลกระทบต่อระบบงานหรือข้อมูลสารสนเทศที่มีความสำคัญหรือมีลักษณะอ่อนไหว เช่น ข้อมูลส่วนบุคคล ข้อมูลด้านสุขภาพ หรือระบบที่มีความสำคัญต่อภารกิจหลักขององค์กร จะต้องผ่านกระบวนการประเมินความเสี่ยงด้านเทคโนโลยีสารสนเทศ (IT Risk Assessment) และการประเมินผลกระทบต่อความต่อเนื่องทางธุรกิจ (Business Impact Assessment: BIA) อย่างเป็นระบบ เพื่อให้สามารถกำหนดมาตรการควบคุมความเสี่ยงและแนวทางรองรับกรณีฉุกเฉินได้อย่างเพียงพอและเหมาะสม

5.6.4 **การใช้หลักวงจรการพัฒนาระบบและแนวทางการพัฒนาระบบที่ปลอดภัย** (System Development Life Cycle and Secure Development Practices)

องค์กรต้องสนับสนุนให้การดำเนินโครงการด้านเทคโนโลยีสารสนเทศเป็นไปตามหลักวงจรชีวิตการพัฒนาระบบ (System Development Life Cycle: SDLC) อย่างครบถ้วน ครอบคลุมทุกขั้นตอนที่สำคัญ ได้แก่ การวิเคราะห์ความต้องการ การวางแผน การออกแบบ การพัฒนา การทดสอบ การนำไปใช้งานจริง และการบำรุงรักษา เพื่อให้สามารถส่งมอบระบบงานที่มีคุณภาพ มีความเสถียร และสามารถตอบสนองต่อความต้องการขององค์กรได้อย่างมีประสิทธิภาพ

รวมทั้งกำหนดให้มีการนำแนวทางการพัฒนาอย่างปลอดภัย (Secure Software Development) มาใช้ตลอดวงจรชีวิตการพัฒนาระบบและสนับสนุนให้มีการฝึกอบรมพัฒนาทักษะด้าน Secure Coding และ Security Testing ให้กับทีมพัฒนาและทีมที่เกี่ยวข้อง พร้อมทั้งกำหนดให้มีการทบทวนซอร์สโค้ด การประเมินช่องโหว่ของระบบและการทดสอบการเจาะระบบอย่างเป็นระบบก่อนนำระบบขึ้นใช้งานจริง เพื่อให้ระบบเทคโนโลยีสารสนเทศที่พัฒนาและนำมาใช้งานภายในองค์กรมีความมั่นคงปลอดภัย เชื่อถือได้ และสอดคล้องกับข้อกำหนดด้านกฎหมาย มาตรฐานสากล และข้อกำหนดจากหน่วยงานกำกับดูแลที่เกี่ยวข้อง

5.6.5 **การติดตามและรายงานผล** (Project Monitoring and Reporting)

องค์กรต้องกำหนดให้มีการติดตามความก้าวหน้า การควบคุมงบประมาณ การจัดการความเสี่ยง และผลลัพธ์ของโครงการอย่างสม่ำเสมอ พร้อมทั้งจัดทำรายงานเพื่อนำเสนอแก่ผู้บริหารหรือคณะกรรมการที่เกี่ยวข้องอย่างเป็นระบบ เพื่อให้สามารถตัดสินใจเชิงกลยุทธ์และกำกับดูแลได้อย่างเหมาะสมและทันท่วงที

5.7 การใช้เทคโนโลยีดิจิทัลและปัญญาประดิษฐ์ (AI) อย่างรับผิดชอบ

บริษัทตระหนักถึงศักยภาพของเทคโนโลยีดิจิทัลและระบบปัญญาประดิษฐ์ (Artificial Intelligence: AI) ในการสนับสนุนการดำเนินงาน การตัดสินใจทางคลินิก การบริหารจัดการ และการให้บริการด้านสุขภาพที่มีประสิทธิภาพ แม่นยำ และสามารถปรับให้เหมาะสมกับลักษณะเฉพาะของผู้รับบริการ (Personalized Healthcare) อย่างไรก็ตาม บริษัทให้ความสำคัญสูงสุดต่อการใช้งานเทคโนโลยีดังกล่าวอย่างมีความรับผิดชอบ โปร่งใส และอยู่ภายใต้หลักจริยธรรม รวมถึงกรอบการกำกับดูแลที่เหมาะสม เพื่อป้องกันความเสี่ยงต่อผู้รับบริการ ข้อมูลสุขภาพส่วนบุคคล และความน่าเชื่อถือขององค์กร

เพื่อให้การนำเทคโนโลยี AI มาใช้งานในองค์กรเป็นไปอย่างมีจริยธรรมและรับผิดชอบ บริษัทจึงกำหนดแนวทางปฏิบัติดังต่อไปนี้

5.7.1 **การใช้เทคโนโลยีอย่างมีจริยธรรม** (Ethical Use of AI)

บริษัทให้ความสำคัญต่อหลักจริยธรรมในการนำเทคโนโลยีปัญญาประดิษฐ์ (AI) มาใช้ในการดำเนินงาน โดยยึดถือแนวทางการใช้ AI อย่างมีความรับผิดชอบ โปร่งใส และเคารพสิทธิมนุษยชน ตามแนวปฏิบัติจริยธรรมปัญญาประดิษฐ์แห่งชาติ และมาตรฐานสากลที่เกี่ยวข้อง การนำระบบ AI มาใช้งานภายในองค์กรจะต้องดำเนินการภายใต้กรอบจริยธรรมที่ครอบคลุมประเด็นสำคัญ ดังนี้

- **ความเป็นธรรม** (Fairness) หลีกเลี่ยงการเลือกปฏิบัติหรืออคติที่อาจเกิดขึ้นจากโมเดล AI โดยเฉพาะในบริบทที่เกี่ยวข้องกับข้อมูลสุขภาพหรือการให้บริการสาธารณสุข

- **ความโปร่งใส** (Transparency) เปิดเผยวัตถุประสงค์ วิธีการทำงาน และข้อจำกัดของระบบ AI ต่อผู้มีส่วนได้เสียอย่างเหมาะสม
- **ความรับผิดชอบ** (Accountability) มีการกำหนดบทบาทและความรับผิดชอบที่ชัดเจนของบุคลากรหรือหน่วยงานที่เกี่ยวข้องกับการพัฒนาและใช้งานระบบ AI
- **ความปลอดภัย** (Safety) รับรองว่าระบบ AI ได้รับการออกแบบ พัฒนา และใช้งานอย่างปลอดภัยต่อทั้งบุคลากร ผู้รับบริการ และโครงสร้างพื้นฐานขององค์กร
- **การเคารพสิทธิมนุษยชน** (Human Rights Respect) ระบบ AI ต้องไม่ละเมิดสิทธิขั้นพื้นฐานของบุคคล และต้องสามารถถูกตรวจสอบและยับยั้งการดำเนินการได้โดยมนุษย์
- **การคุ้มครองข้อมูลส่วนบุคคล** (Privacy) การเก็บ ใช้ และเผยแพร่ข้อมูลในระบบ AI ต้องเป็นไปตามหลักการของพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 และข้อกำหนดด้านความมั่นคงปลอดภัยของข้อมูล (Data Security)

นอกจากนี้ บริษัทกำหนดให้ระบบ AI ที่นำมาใช้ โดยเฉพาะในกระบวนการที่เกี่ยวข้องกับการวินิจฉัย การตัดสินใจทางคลินิก หรือมีผลกระทบต่อชีวิตและสุขภาพของผู้รับบริการ จะต้องมีคุณสมบัติด้านการอธิบายได้ (Explainability) ในระดับที่เหมาะสม และสามารถเปิดเผยเหตุผลเบื้องหลังการตัดสินใจของระบบได้อย่างชัดเจนต่อบุคลากรที่เกี่ยวข้อง เพื่อเสริมสร้างความเชื่อมั่น ความโปร่งใส และความสามารถในการตรวจสอบย้อนหลัง (Auditability) ได้อย่างมีประสิทธิภาพ

เพื่อให้มั่นใจว่าการตัดสินใจที่เกิดจากระบบ AI มีความถูกต้อง เหมาะสม และสามารถตรวจสอบได้ บริษัทกำหนดให้มีการออกแบบระบบ AI โดยผนวกแนวคิดการมีส่วนร่วมของมนุษย์ในกระบวนการตัดสินใจ (Human Oversight หรือ Human-in-the-loop) ตามลักษณะความเสี่ยงของระบบ AI ดังนี้

- ระบบที่มีผลกระทบสูงต่อชีวิต ความปลอดภัย หรือสิทธิของบุคคล เช่น ระบบช่วยวินิจฉัยโรค การจัดลำดับผู้ป่วย หรือการประเมินผลทางคลินิก ต้องอยู่ภายใต้การกำกับโดยตรงของบุคลากรที่มีอำนาจในการอนุมัติหรือปฏิเสธผลลัพธ์ที่ได้จากระบบ AI
- ต้องมีการออกแบบระบบให้สามารถแจ้งเตือนหรือยับยั้งการดำเนินการอัตโนมัติ (Override) ได้โดยมนุษย์เมื่อพิจารณาว่าข้อมูลหรือผลลัพธ์จาก AI อาจมีความผิดพลาดหรือไม่สอดคล้องกับบริบท
- มีการกำหนดแนวทางการฝึกอบรมและเพิ่มพูนทักษะให้แก่บุคลากรที่เกี่ยวข้องกับการใช้งานระบบ AI เพื่อให้สามารถทำหน้าที่เป็นผู้ตรวจสอบ ทบทวน หรือผู้ตัดสินใจสุดท้าย (Human Reviewer / Final Arbiter) ได้อย่างมีประสิทธิภาพ
- จัดให้มีการบันทึกและจัดเก็บหลักฐานในการมีส่วนร่วมของมนุษย์ในแต่ละขั้นตอน เพื่อใช้ในการตรวจสอบภายหลัง (Audit Trail)

5.7.2 การประเมินความเสี่ยงและผลกระทบจากการใช้ AI (AI Risk and Impact Assessment)

- ก่อนการนำ AI หรือ ML มาใช้งานในระบบสารสนเทศหรือกระบวนการทางธุรกิจขององค์กร หน่วยงานที่เกี่ยวข้องต้องดำเนินการประเมินผลกระทบ (AI Impact Assessment) และการประเมินความเสี่ยง (AI Risk

Assessment) อย่างรอบด้าน โดยครอบคลุมถึงผลกระทบด้านความมั่นคงปลอดภัยของข้อมูล ความเป็นส่วนตัวของข้อมูล (Privacy) และสิทธิเสรีภาพของผู้ใช้บริการหรือผู้มีส่วนได้ส่วนเสีย

- สำหรับระบบ AI ที่จัดอยู่ในระดับความเสี่ยงสูง (High-risk AI) เช่น ระบบช่วยวินิจฉัยโรค หรือการจัดลำดับความสำคัญของผู้ป่วย จะต้องได้รับความเห็นชอบจากคณะกรรมการที่เกี่ยวข้องก่อนใช้งานจริง

5.7.3 **การจัดตั้งคณะกรรมการกำกับดูแลจริยธรรม AI (AI Ethics Governance Board)**

- เพื่อให้การพัฒนาและการใช้งานเทคโนโลยีปัญญาประดิษฐ์ (Artificial Intelligence – AI) ภายในองค์กรเป็นไปอย่างมีจริยธรรม โปร่งใส และสอดคล้องกับกฎหมาย มาตรฐานสากล และแนวทางกำกับดูแลที่เกี่ยวข้อง องค์กรต้องจัดให้มีคณะกรรมการหรือคณะทำงานระดับองค์กร เพื่อทำหน้าที่กำหนดนโยบาย แนวทาง และมาตรฐานจริยธรรมที่เกี่ยวข้องกับการพัฒนาและใช้งาน AI ในทุกระดับขององค์กร

5.7.4 **การควบคุมและตรวจสอบระบบ AI (AI Model Governance and Monitoring)**

- ต้องมีแนวทางรองรับกรณีที่ผู้ใช้งานร้องขอให้มีการอธิบายผลลัพธ์ หรือปฏิเสธการตัดสินใจที่มาจาก AI อย่างชัดเจน
- องค์กรต้องกำหนดให้มีการจัดเก็บ metadata และข้อมูลอ้างอิงที่สำคัญของระบบ AI ทุกระบบ เช่น เวอร์ชั่นของโมเดล ข้อมูลที่ใช้ในการฝึก ระบบที่เชื่อมโยง และผลลัพธ์จากการทดสอบ
- ระบบ AI จะต้องมีการกำกับดูแลและตรวจสอบผลลัพธ์อย่างสม่ำเสมอ (Performance Monitoring) ในกรณีที่ตรวจพบการเปลี่ยนแปลงของพฤติกรรมโมเดล (Model Drift) หรือความเบี่ยงเบนของผลลัพธ์ ต้องดำเนินการวิเคราะห์สาเหตุและปรับปรุงโมเดลโดยทันที เช่น การรีเทรน (Retraining) การปรับพารามิเตอร์ หรือการเปลี่ยนแปลงข้อมูลฝึกสอน เพื่อป้องกันความเสี่ยงที่อาจเกิดขึ้นจากการตัดสินใจของระบบ AI
- โมเดลที่มีความสำคัญเชิงกลยุทธ์ หรือใช้ในกระบวนการตัดสินใจที่มีผลกระทบต่อบุคคล ต้องได้รับการตรวจสอบโดยผู้เชี่ยวชาญอิสระก่อนนำมาใช้งาน

5.7.5 **ความสอดคล้องกับกฎหมายและมาตรฐาน (Legal and Regulatory Compliance)**

- การใช้ AI ต้องเป็นไปตามกฎหมายที่เกี่ยวข้อง ได้แก่ พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 (PDPA) และมาตรฐานสากล เช่น ISO/IEC 23894:2023, NIST AI Risk Management Framework
- ต้องมีการจัดทำบันทึกการประเมินผลกระทบและความเสี่ยง และเปิดเผยนโยบายการใช้ AI ต่อสาธารณชนหรือหน่วยงานกำกับดูแลตามความเหมาะสม

6. **การวัด ติดตาม วิเคราะห์และประเมินผล (Performance Monitoring and Evaluation)**

บริษัทกำหนดให้มีการวัดผล ติดตาม วิเคราะห์ และประเมินผลการกำกับดูแลและบริหารจัดการเทคโนโลยีสารสนเทศอย่างต่อเนื่องและเป็นระบบ เพื่อให้มั่นใจว่ากระบวนการที่ดำเนินการอยู่มีประสิทธิภาพ สอดคล้องกับกลยุทธ์องค์กร และสามารถตอบสนองต่อการเปลี่ยนแปลงของสภาพแวดล้อมทางธุรกิจ เทคโนโลยี และภัยคุกคามได้อย่างเหมาะสม

การประเมินผลจะครอบคลุมทั้งมุมมองเชิงกลยุทธ์ เชิงปฏิบัติการ และเชิงการควบคุมภายใน โดยใช้ดัชนีชี้วัด (KPIs) ตัวชี้วัดความเสี่ยง (KRIs) และกลไกการตรวจสอบตามแนวปฏิบัติที่องค์กรกำหนด พร้อมทั้งรายงานผลการประเมินต่อคณะกรรมการหรือผู้มีอำนาจตามลำดับ เพื่อใช้ประกอบการปรับปรุงและตัดสินใจเชิงนโยบายอย่างต่อเนื่อง

7. **การสื่อสารและการฝึกอบรม** (Awareness and Training)

บริษัทตระหนักถึงความสำคัญของการเสริมสร้างความรู้ ความเข้าใจ และพฤติกรรมที่เหมาะสมของบุคลากรในทุกระดับเกี่ยวกับบทบาท หน้าที่ และความรับผิดชอบภายใต้กรอบการกำกับดูแลและบริหารจัดการเทคโนโลยีสารสนเทศ เพื่อให้สามารถสนับสนุนการบรรลุวัตถุประสงค์ด้านกำกับดูแลและบริหารจัดการเทคโนโลยีสารสนเทศ (IT Governance) ได้อย่างมีประสิทธิภาพ โปร่งใส และสามารถตรวจสอบได้

เพื่อสนับสนุนการดำเนินงานตามนโยบายการกำกับดูแลและบริหารจัดการเทคโนโลยีสารสนเทศ บริษัทกำหนดให้มีการดำเนินการด้านการสื่อสารและฝึกอบรมตามแนวทางต่อไปนี้

7.1 จัดให้มีการเผยแพร่ความรู้และสร้างความเข้าใจเกี่ยวกับหลักการของการกำกับดูแลและบริหารจัดการเทคโนโลยีสารสนเทศ รวมถึงโครงสร้าง บทบาทหน้าที่ของคณะกรรมการและคณะทำงานที่เกี่ยวข้อง ตลอดจนกระบวนการตัดสินใจในระดับนโยบายและการดำเนินงาน

7.2 ดำเนินการสื่อสารนโยบาย มาตรฐาน แนวปฏิบัติ และข้อกำหนดทางกฎหมาย หรือกฎระเบียบที่เกี่ยวข้องกับการใช้เทคโนโลยีสารสนเทศ ให้แก่บุคลากรในทุกระดับอย่างทั่วถึงและต่อเนื่อง

7.3 กำหนดให้มีการจัดการฝึกอบรมเชิงระบบอย่างสม่ำเสมอแก่พนักงาน ผู้บริหาร และหน่วยงานที่เกี่ยวข้อง เพื่อยกระดับความตระหนักรู้ ทักษะ และสมรรถนะในการปฏิบัติงานให้สอดคล้องกับกรอบการกำกับดูแลเทคโนโลยีสารสนเทศขององค์กร

7.4 พัฒนาและปรับปรุงเนื้อหาหลักสูตรการฝึกอบรมให้สอดคล้องกับบทบาทและความรับผิดชอบของแต่ละกลุ่มเป้าหมาย อาทิ ผู้ใช้งานทั่วไป เจ้าของระบบ ผู้บริหารโครงการ หรือเจ้าหน้าที่กำกับดูแลความมั่นคงปลอดภัยสารสนเทศ

7.5 กำหนดให้มีการประเมินผลการฝึกอบรม และทบทวนเนื้อหาอย่างน้อยปีละหนึ่งครั้ง เพื่อให้ทันต่อการเปลี่ยนแปลงของเทคโนโลยี สภาพแวดล้อมทางธุรกิจ และกฎระเบียบที่เกี่ยวข้อง

8. **การทบทวนและปรับปรุงนโยบาย** (Policy Review and Updates)

บริษัทตระหนักถึงความสำคัญของการทบทวนและปรับปรุงนโยบายการกำกับดูแลและบริหารจัดการเทคโนโลยีสารสนเทศอย่างสม่ำเสมอ เพื่อให้มั่นใจว่านโยบายดังกล่าวยังคงมีความเหมาะสม ทันสมัย และสอดคล้องกับแนวปฏิบัติที่ดี มาตรฐานสากล ข้อกำหนดทางกฎหมาย และบริบทด้านเทคโนโลยีที่เปลี่ยนแปลงไป โดยกำหนดให้มีการทบทวนหรือปรับปรุงนโยบายอย่างน้อยปีละหนึ่งครั้งหรือเมื่อมีเหตุการณ์สำคัญที่อาจส่งผลกระทบต่อการกำกับดูแลและบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศ ทั้งนี้ เพื่อให้แนวทางการดำเนินงานขององค์กรมีความสอดคล้องกับสถานการณ์ปัจจุบันและสามารถรองรับความเสี่ยงที่อาจเกิดขึ้นได้อย่างเหมาะสมและทันท่วงที

การทบทวนนโยบายต้องดำเนินการโดยหน่วยงานที่รับผิดชอบหลักร่วมกับหน่วยงานที่กำกับดูแลสารสนเทศและต้องได้รับการอนุมัติจากผู้บริหารระดับสูงหรือคณะกรรมการที่เกี่ยวข้องก่อนนำไปบังคับใช้ โดยผลจากการทบทวนต้องถูกบันทึกอย่างเป็นทางการและใช้เป็นข้อมูลประกอบในการพัฒนาหรือปรับปรุงกระบวนการบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศอย่างต่อเนื่อง เพื่อให้มั่นใจว่านโยบายยังคงมีความเหมาะสม สอดคล้อง และตอบสนองต่อบริบทที่เปลี่ยนแปลงได้อย่างมีประสิทธิภาพ

9. **การบังคับใช้และบทลงโทษ** (Enforcement and Penalties)

บริษัทกำหนดให้บุคลากรทุกระดับต้องปฏิบัติตามนโยบาย มาตรการ ขั้นตอนการปฏิบัติงาน และแนวทางที่อยู่ภายใต้กรอบภายใต้กรอบการกำกับดูแลและบริหารจัดการเทคโนโลยีสารสนเทศ อย่างเคร่งครัด ทั้งนี้เพื่อให้การบริหารจัดการระบบเทคโนโลยีสารสนเทศ ระบบเครือข่าย และโครงสร้างพื้นฐานดิจิทัลขององค์กรเป็นไปอย่างมีประสิทธิภาพ ปลอดภัย และสามารถตรวจสอบได้

การกระทำใด ๆ อันเป็นการละเมิด ฝ่าฝืน ละเลย ไม่ปฏิบัติตามนโยบาย มาตรการ ขั้นตอน แนวทางปฏิบัติที่กำหนดไว้หรือเอกสารที่เกี่ยวข้องกับการกำกับดูแลและบริหารจัดการเทคโนโลยีสารสนเทศขององค์กร หรือปฏิบัติอย่างไม่เหมาะสม ไม่ว่าจะโดยเจตนา หรือประมาทเลินเล่อ ที่อาจส่งผลให้เกิดความเสี่ยงต่อความมั่นคงปลอดภัยของระบบสารสนเทศ ตลอดจนกระทบต่อความต่อเนื่องทางธุรกิจ ชื่อเสียง และความเชื่อมั่นของผู้มีส่วนได้ส่วนเสีย บริษัทจะดำเนินการตามมาตรการทางวินัยที่กำหนดไว้ในระเบียบหรือข้อบังคับของบริษัท กรุงเทพดุสิตเวชการ จำกัด (มหาชน) หรือบทลงโทษอื่นใดตามที่ระบุไว้ในข้อบังคับขององค์กร นโยบายด้านทรัพยากรบุคคล และ/หรือกฎหมายที่เกี่ยวข้อง

ในกรณีที่เป็นบุคคลภายนอก เช่น คู่สัญญา ผู้รับจ้าง หรือพันธมิตรทางธุรกิจ องค์กรอาจดำเนินการยกเลิกสัญญา ยุติความร่วมมือ หรือดำเนินการทางกฎหมายตามที่กำหนดไว้ในข้อตกลง

10. เอกสารอ้างอิง (Reference)

1. International Organization for Standardization. (2016). *ISO 27799:2016 — Health informatics — Information security management in health using ISO/IEC 27002*. Geneva, Switzerland: ISO.
2. International Organization for Standardization & International Electrotechnical Commission. (2021). *ISO/IEC 27036 — Information security for supplier relationships (Parts 1–4)*. Geneva, Switzerland: ISO/IEC.
3. International Organization for Standardization & International Electrotechnical Commission. (2022). *ISO/IEC 27001:2022 — Information security, cybersecurity and privacy protection — Information security management systems — Requirements*. Geneva, Switzerland: ISO/IEC.
4. International Organization for Standardization & International Electrotechnical Commission. (2023). *ISO/IEC 23894:2023 — Artificial intelligence — Risk management*. Geneva, Switzerland: ISO/IEC.
5. ISACA. (2018). *COBIT® 2019 framework: Governance and management objectives*. ISACA.
6. National Institute of Standards and Technology. (2023). *Artificial intelligence risk management framework (AI RMF 1.0)*. U.S. Department of Commerce.
7. Securities and Exchange Commission, Thailand. (2023, December). *Artificial intelligence in capital market – Governance framework*. Bangkok, Thailand: SEC Thailand.
8. สำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์. (2562). *แนวทางการกำกับดูแลและบริหารจัดการเทคโนโลยีสารสนเทศระดับองค์กรที่ดี (IT Governance Practice)*.
9. สำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์. (2566). *กรอบการกำกับดูแลการใช้งานปัญญาประดิษฐ์ (AI) และการเรียนรู้ของเครื่อง (ML) ในตลาดทุน*. กรุงเทพฯ: สำนักงาน ก.ล.ต.
10. สำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์. (2567). *การกำกับดูแลและบริหารจัดการด้านเทคโนโลยีสารสนเทศ (Information Technology Governance) (แนบท้ายประกาศ สธ. 33/2567)*.
11. สำนักงานคณะกรรมการดิจิทัลเพื่อเศรษฐกิจและสังคมแห่งชาติ. (2564). *แนวปฏิบัติจริยธรรมปัญญาประดิษฐ์แห่งชาติ (Thailand AI Ethics Guideline)*.
12. พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562. (2562).

11. เอกสารที่เกี่ยวข้อง (Related documents)

1. เอกสารแนบท้าย 1: รายชื่อบริษัท กรุงเทพดุสิตเวชการ จำกัด (มหาชน) และบริษัทย่อย

2. นโยบายการบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศ (IT Risk Management Policy)
3. นโยบายการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ (Information Security Management Policy)

12. เอกสารแนบท้าย 1: รายชื่อบริษัท กรุงเทพดุสิตเวชการ จำกัด (มหาชน) และบริษัทย่อย

1. ธุรกิจโรงพยาบาลเอกชน (Healthcare Business)

   https://investor.bdms.co.th/th/general/bdms-at-a-glance

   20250513-bdms-he
   althcare-business-th

2. ธุรกิจที่เกี่ยวเนื่องกับการรักษาพยาบาล (Business Related to Medical Services

   https://investor.bdms.co.th/th/general/bdms-at-a-glance

   20240313-businessr
   elated-to-medicalse