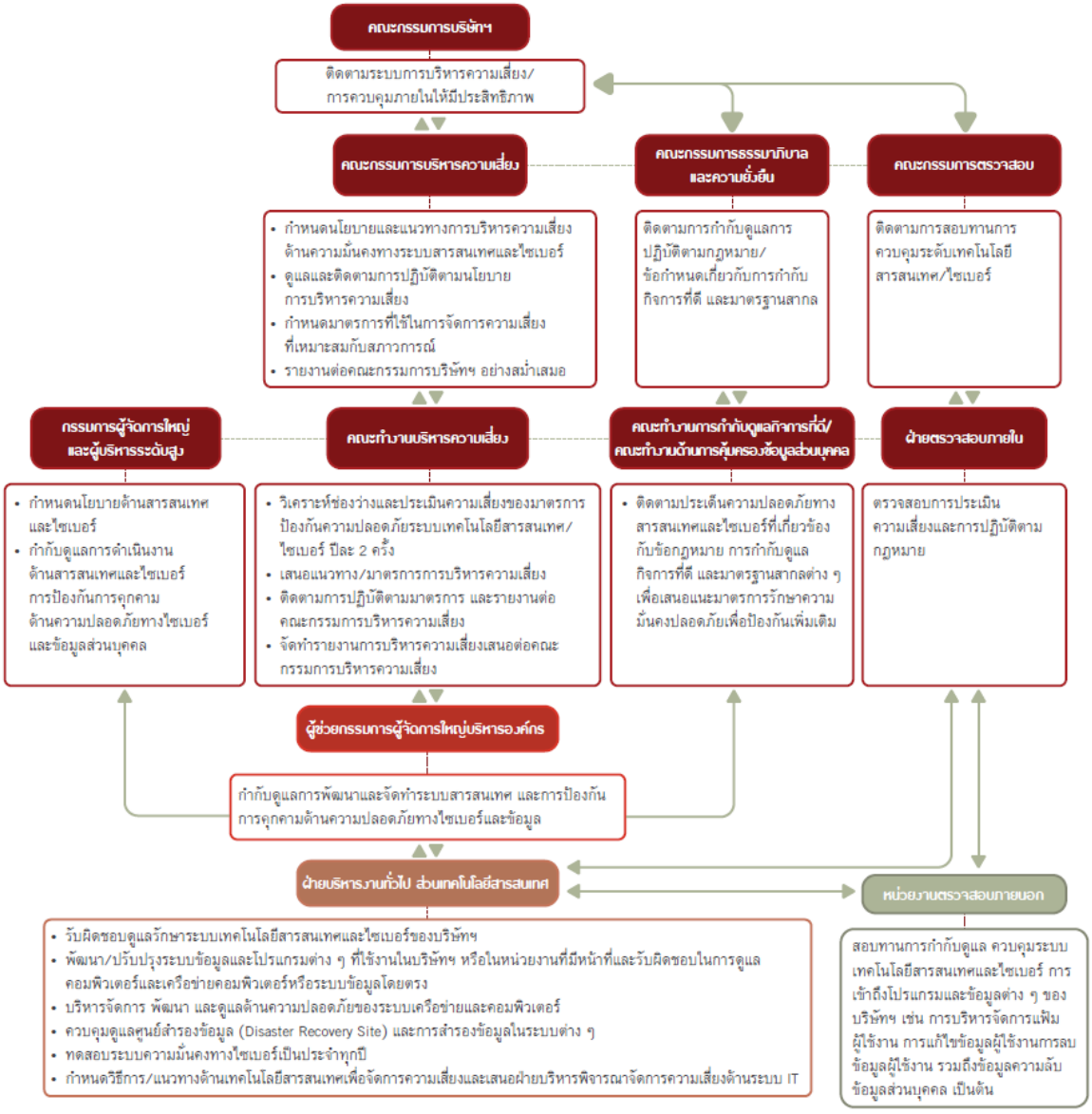
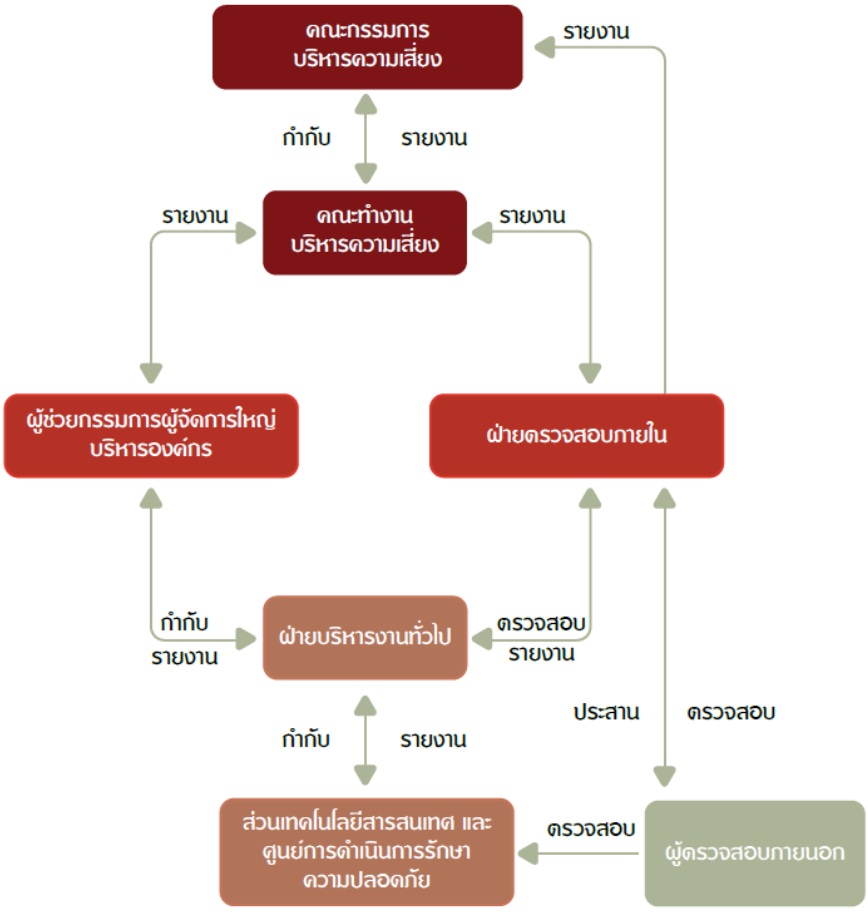
ความมั่นคงปลอดภัยสารสนเทศและไซเบอร์

ประเด็นด้านการถูกโจมตีทางไซเบอร์ (Cyberattacks) เป็นประเด็นความเสี่ยงที่สำคัญของโลก ตามรายงานของ World Economic Forum 2024 และยังถูกประเมินให้เป็นความเสี่ยงของบริษัทฯ ที่อาจสร้างผลกระทบต่อการดำเนินธุรกิจ บริษัทฯ จึงให้ความสำคัญกับการรักษาความมั่นคงปลอดภัยทางไซเบอร์ รวมทั้งระบบเทคโนโลยีสารสนเทศขององค์กร เพื่อให้มั่นใจว่าบริษัทฯ สามารถดำเนินธุรกิจได้อย่างต่อเนื่อง และข้อมูลของบริษัทฯ ได้รับการปกป้องคุ้มครองไว้เป็นอย่างดี ทั้งนี้ บริษัทฯ ได้จัดให้มีส่วนเทคโนโลยีสารสนเทศ ภายใต้สายงานบริหารองค์กร เป็นหน่วยงานรับผิดชอบจัดการระบบเทคโนโลยีสารสนเทศและป้องกัน รวมถึงการป้องกันข้อมูลและระบบจากภัยคุกคามทางไซเบอร์ขององค์กร พร้อมทั้งประกาศใช้นโยบาย/แนวทางปฏิบัติด้านสารสนเทศและไซเบอร์ เพื่อรักษาศักยภาพและขีดความสามารถทางธุรกิจของบริษัทฯ รวมทั้งความเชื่อมั่นของผู้มีส่วนได้เสีย ด้วย

โครงสร้างการกำกับดูแลด้านความมั่นคงปลอดภัยสารสนเทศและไซเบอร์



กระบวนการติดตามตรวจสอบความมั่นคงของระบบสารสนเทศ



บทบาทหน้าที่

คณะทำงานบริหารความเสี่ยง	ติดตามมาตรการป้องกันความปลอดภัยระบบเทคโนโลยีสารสนเทศและไซเบอร์ ปีละ 2 ครั้ง
ฝ่ายตรวจสอบภายใน	1. การสอบทานเกี่ยวกับการปฏิบัติตามนโยบาย/ระเบียบปฏิบัติต่าง ๆ ดังนี้ • นโยบายความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ • ประสิทธิภาพและความเพียงพอในการจัดการความเสี่ยงด้านสารสนเทศและระบบรักษาความปลอดภัยของระบบสารสนเทศและข้อมูล • แผนฉุกเฉินสำหรับป้องกันความปลอดภัยของระบบสารสนเทศเมื่อมีอุบัติภัยร้ายแรง • การซ้อมแผนฉุกเฉินตามแผนการบริหารความต่อเนื่องทางธุรกิจของบริษัทฯ • มาตรการป้องกันระบบรักษาความปลอดภัยอุปกรณ์คอมพิวเตอร์ • การประเมินความเสี่ยงด้านความปลอดภัยของระบบเทคโนโลยีและสารสนเทศ 2. รายงานด้านการเฝ้าระวังภัยคุกคามผ่านระบบเครือข่ายคอมพิวเตอร์ เป็นประจำทุกปี
ส่วนเทคโนโลยีสารสนเทศและศูนย์การดำเนินการรักษาความปลอดภัย	ติดตาม ตรวจหา คัดกรอง ป้องกัน และตอบสนองต่อภัยคุกคามทางไซเบอร์ที่อาจเกิดขึ้น ทั้งจากภายในและภายนอกองค์กรอย่างต่อเนื่อง รวมทั้งการรายงานของระบบต่าง ๆ เช่นระบบป้องกันผู้บุกรุกระบบไฟร์วอลล์และระบบป้องกันภัยคุกคามทางอินเทอร์เน็ต เป็นต้น
ผู้ตรวจสอบภายนอก	สอบทานการควบคุมของระบบเทคโนโลยีสารสนเทศ การเข้าถึงโปรแกรมและข้อมูล เช่น การบริหารจัดการแฟ้มผู้ใช้งานทั้งการแก้ไข/ลบข้อมูลผู้ใช้งานเพื่อประกอบในการสอบทานงบการเงินของบริษัทฯโดยดำเนินการเป็นประจำทุกปี

ความเสี่ยงด้านเทคโนโลยีสารสนเทศและไซเบอร์

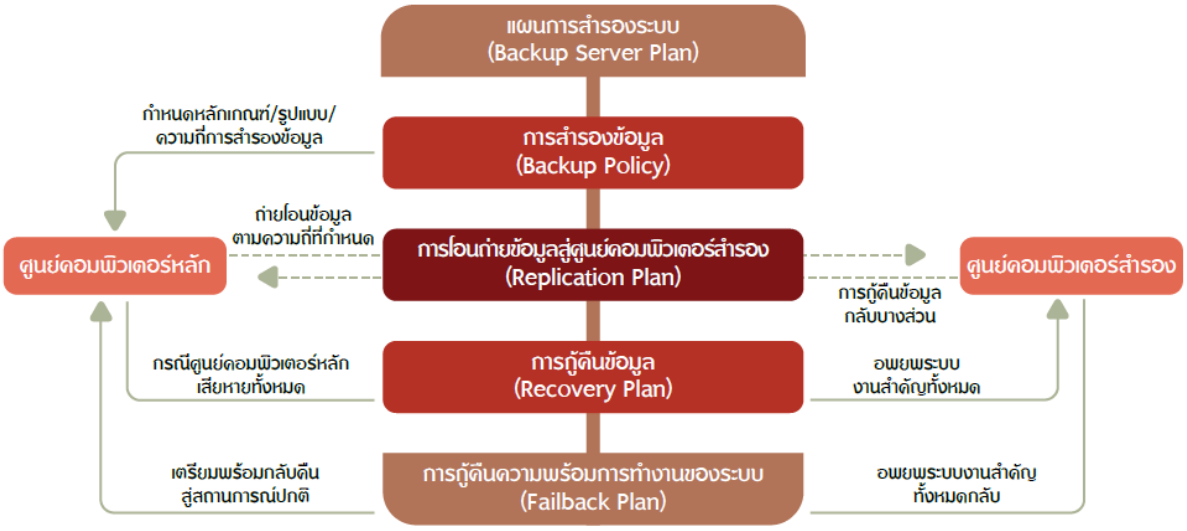
บริษัทฯ ได้ประเมินและวิเคราะห์ความเสี่ยงด้านเทคโนโลยีสารสนเทศและไซเบอร์ ซึ่งถือเป็นหนึ่งในความเสี่ยงสำคัญของบริษัทฯ พร้อมกำหนดมาตรการควบคุมไว้อย่างชัดเจน

ปัจจัยเสี่ยง: ด้านกายภาพและสภาพแวดล้อม	**ระดับความเสี่ยงคงเหลือ:** ต่ำ
ลักษณะความเสี่ยง: การเข้า-ออก ใช้งาน และตรวจสอบระบบของห้อง Data Center ที่ติดตั้งเครื่องคอมพิวเตอร์แม่ข่าย (Server) ของบุคลากรภายในและภายนอก	
มาตรการควบคุม: • ติดตั้งระบบป้องกันผู้บุกรุก และระบบสแกนนิ้วมือที่จำกัดเฉพาะเจ้าหน้าที่ที่ได้รับอนุญาตเท่านั้น รวมถึงควบคุมการเข้า-ออกของบุคลากรภายนอกผู้ให้บริการด้านต่าง ๆ ของห้อง Data Center พร้อมตรวจสอบข้อมูลการเข้า-ออกเป็นประจำทุกเดือน • จัดให้มีการตรวจสอบจากฝ่ายตรวจสอบภายใน และหน่วยงานตรวจสอบภายนอกด้วย	
ปัจจัยเสี่ยง: การใช้งานโปรแกรมคอมพิวเตอร์บนเครื่องคอมพิวเตอร์ของบริษัทฯ	**ระดับความเสี่ยงคงเหลือ:** ต่ำ
ลักษณะความเสี่ยง: การติดตั้งโปรแกรมที่ไม่ปลอดภัยหรือไม่ประสงค์ดี ทั้งโดยตั้งใจและไม่ตั้งใจของผู้ปฏิบัติงาน	
มาตรการควบคุม: • กำหนดเป็นระเบียบการใช้งานระบบเครือข่ายและคอมพิวเตอร์ • ติดตั้งระบบไฟร์วอลล์ ซอฟต์แวร์ Endpoint Protection และ Data Inventory เพื่อป้องกัน Malware ต่าง ๆ และตรวจสอบการใช้งาน • สร้างความตระหนักเกี่ยวกับการติดตั้งโปรแกรมที่นอกเหนือจากที่บริษัทฯ จัดให้ต่อพนักงานอย่างสม่ำเสมอ พร้อมระบุบทลงโทษกรณีมีการกระทำผิดด้วย	
ปัจจัยเสี่ยง: การใช้งานระบบเครือข่ายคอมพิวเตอร์ของบริษัทฯ	**ระดับความเสี่ยงคงเหลือ:** ต่ำ
ลักษณะความเสี่ยง: การเข้าถึงหรือโจมตีระบบเครือข่ายจากภายนอก	
มาตรการควบคุม: • จัดให้มีระบบป้องกันภัยคุกคามทางอินเทอร์เน็ตภายในองค์กร เพื่อป้องกันการเข้าถึง/โจมตี Server และคอมพิวเตอร์ของพนักงาน • จัดให้มีศูนย์ปฏิบัติการเฝ้าระวังความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ (Security Operation Center: SOC) ทำหน้าที่เฝ้าระวังและป้องกันการคุกคามระบบ/อุปกรณ์ของบริษัทฯ จากภายนอก โดยใช้ระบบ AI/บุคลากร ดำเนินการตลอด 24 ชั่วโมง	
ปัจจัยเสี่ยง: ด้านบุคคลที่เกิดจากการจัดการสิทธิที่ไม่เหมาะสม	**ระดับความเสี่ยงคงเหลือ:** ต่ำ
ลักษณะความเสี่ยง: การเข้าถึงและแก้ไขข้อมูลของบุคคลที่ไม่ได้รับสิทธิให้เข้าถึงหรือจัดการข้อมูล	
มาตรการควบคุม: กำหนดสิทธิการเข้าถึงและใช้งานระบบเครื่องคอมพิวเตอร์ พร้อมระบบป้องกันผู้บุกรุก	
ปัจจัยเสี่ยง: ภัยและสถานการณ์ฉุกเฉิน	**ระดับความเสี่ยงคงเหลือ:** ต่ำ
ลักษณะความเสี่ยง: ภัยพิบัติ ภัยธรรมชาติ การเกิดกระแสไฟฟ้าขัดข้อง การชุมนุมประท้วง ที่อาจทำให้เกิดความไม่ต่อเนื่องในการทำงาน/การดำเนินธุรกิจ	
มาตรการควบคุม: กำหนดแผนรองรับเหตุภัยพิบัติของระบบงานเทคโนโลยีสารสนเทศ และแผนความต่อเนื่องทางธุรกิจ เพื่อรองรับเหตุฉุกเฉิน พร้อมกำหนดให้มีการทบทวนและซ้อมแผนเป็นประจำทุกปี	
ปัจจัยเสี่ยง: ความไม่สอดคล้องในการบริหารจัดการ	**ระดับความเสี่ยงคงเหลือ:** กลาง
ลักษณะความเสี่ยง: นโยบายและแนวปฏิบัติไม่สอดคล้องกับความเสี่ยง/สถานการณ์ที่อาจจะเกิดขึ้นในอนาคต	
มาตรการควบคุม: • ประเมินความเสี่ยง โอกาส ผลกระทบ ทิศทาง แนวโน้มการเปลี่ยนแปลง ทั้งในด้านเทคนิค ผู้ปฏิบัติงาน และสถานการณ์ฉุกเฉิน • ทบทวนนโยบาย/แนวปฏิบัติ แผนรับมือเหตุฉุกเฉินให้สอดคล้องกับสถานการณ์ปัจจุบันเป็นประจำทุกปี • อบรมให้ความรู้เพื่อสร้างความตระหนักเกี่ยวกับนโยบาย แนวปฏิบัติ และการป้องกันภัยคุกคามทางไซเบอร์ • ทดสอบระบบสำรองข้อมูล และระบบ SAP โดยหน่วยงายภายในและภายนอก • ทวนสอบการควบคุม/ป้องกันระบบสารสนเทศ โดยบริษัทภายนอก	

ปัจจัยเสี่ยง: การบริหารจัดการเทคโนโลยี AI	ระดับความเสี่ยงคงเหลือ: กลาง
ลักษณะความเสี่ยง: การใช้งานเทคโนโลยี AI ที่ไม่เหมาะสมและไม่มีการควบคุม เกิดความไม่ปลอดภัยหรือการรั่วไหลจากการใช้งาน	
มาตรการควบคุม: • อบรมให้ความรู้แก่พนักงาน เพื่อสร้างความตระหนักเกี่ยวกับการใช้เทคโนโลยี AI ให้ถูกต้องและปลอดภัย • กำหนดนโยบาย/แนวทางปฏิบัติการใช้งานเทคโนโลยี AI • พัฒนาระบบการใช้งานเทคโนโลยี AI อย่างเป็นระบบ ปลอดภัย และตรวจสอบได้	

การตอบสนองเหตุภัยพิบัติและเหตุฉุกเฉินระบบงานสารสนเทศและความปลอดภัยทางไซเบอร์

เพื่อเป็นการเตรียมความพร้อมและรับมือต่อเหตุการณ์ฉุกเฉิน ที่ส่งผลกระทบต่อสมรรถนะและประสิทธิภาพของระบบเทคโนโลยีสารสนเทศ บริษัทฯ ได้จัดตั้งศูนย์คอมพิวเตอร์สำรองและจัดทำแผนการรองรับเหตุภัยพิบัติและเหตุฉุกเฉินระบบงานเทคโนโลยีสารสนเทศ โดยมีกระบวนการทำงาน ดังนี้



กระบวนการการแจ้งเหตุเพื่อรายงานเหตุการณ์ด้าน IT/ Cyber/ AI