

จัดทำโดย

Apichaya P.

น.ส.อภิษฎา พงษ์ปรีชา

แผนกบริหารความเสี่ยง

สอบทานโดย



นายเชิดพงษ์ สิริวิเศษ

ประธานกรรมการบริหารความเสี่ยง

อนุมัติโดย



นายประเสริฐ บุญสัมพันธ์

ประธานกรรมการ

1. บทนำ (Introduction)

บริษัท ไทยโรเทคไทย เอเยนซีส์ จำกัด (มหาชน) (“บริษัทฯ”) ตระหนักถึงความสำคัญของการดำเนินธุรกิจอย่างต่อเนื่องและความสามารถในการรับมือกับเหตุการณ์หรืออุบัติการณ์ที่อาจทำให้การดำเนินธุรกิจเกิดการหยุดชะงัก ไม่ว่าจะเป็นเนื่องจากปัจจัยภายในหรือภายนอกบริษัทฯ จึงได้กำหนดนโยบายการบริหารความต่อเนื่องทางธุรกิจ (Business Continuity Management Policy: BCMP) เพื่อเป็นกรอบในการป้องกัน เตรียมความพร้อม ตอบสนอง และฟื้นคืนการดำเนินงานที่สำคัญให้กลับสู่ภาวะปกติหรือระดับที่บริษัทฯ กำหนดด้วยยอมรับได้ภายในระยะเวลาที่เหมาะสมได้อย่างมีประสิทธิภาพ ภายใต้การบริหารจัดการความเสี่ยงอย่างเหมาะสม และสอดคล้องกับเป้าหมายทางธุรกิจ กฎหมาย และความคาดหวังของผู้มีส่วนได้เสีย

2. วัตถุประสงค์ความต่อเนื่องทางธุรกิจ (Business Continuity Objective)

- เพื่อให้มีการเตรียมพร้อมรับมือกับภาวะวิกฤตหรือภัยคุกคามต่าง ๆ ที่อาจส่งผลให้การดำเนินงานหยุดชะงัก และสามารถกู้คืนกระบวนการทำงานที่สำคัญได้ตามระยะเวลาที่กำหนด รวมถึงสามารถให้บริการและตอบสนองความต้องการของผู้มีส่วนได้เสียได้อย่างต่อเนื่อง
- เพื่อให้ระบบการบริหารความต่อเนื่องทางธุรกิจ (Business Continuity Management System: BCMS) ของบริษัทฯ มีการพัฒนาและปรับปรุงให้สอดคล้องกับมาตรฐานสากล และทันต่อสถานการณ์ทั้งภายในและภายนอกที่เปลี่ยนแปลงไป
- เพื่อสร้างความรู้ความเข้าใจเกี่ยวกับการดำเนินงานตามระบบการบริหารความต่อเนื่องทางธุรกิจ (Business Continuity Management System: BCMS) ให้กับผู้มีส่วนได้เสียที่สำคัญของบริษัทฯ
- เพื่อสร้างความตระหนักถึงความสำคัญของระบบการบริหารความต่อเนื่องทางธุรกิจ (Business Continuity Management System: BCMS) ให้กับผู้บริหารและพนักงานทุกคน อันจะนำไปสู่การมีส่วนร่วมสนับสนุน และปฏิบัติตามนโยบายการบริหารความต่อเนื่องทางธุรกิจ (Business Continuity Management Policy: BCMP) ของบริษัทฯ เพื่อให้สามารถบรรลุตามวัตถุประสงค์ได้อย่างถูกต้องและทันต่อเหตุการณ์ ภายใต้การคำนึงถึงสวัสดิภาพและความปลอดภัยเป็นสำคัญ
- เพื่อให้ระบบการบริหารความต่อเนื่องทางธุรกิจ (Business Continuity Management System: BCMS) ของบริษัทฯ ที่จัดเตรียมไว้ สามารถนำไปปฏิบัติได้อย่างมีประสิทธิภาพ โดยผู้บริหาร พนักงานทุกคนสามารถปฏิบัติตามหน้าที่และบทบาทที่กำหนดไว้ตามระบบการบริหารความต่อเนื่องทางธุรกิจ (Business Continuity Management System: BCMS) ได้อย่างครบถ้วนและถูกต้อง รวมถึงมีการทบทวนและปรับปรุงระบบดังกล่าวให้เป็นปัจจุบันอย่างสม่ำเสมอ เพื่อให้กระบวนการดำเนินงานที่สำคัญ รวมถึงบุคลากร สถานที่ปฏิบัติงาน ระบบเทคโนโลยีสารสนเทศ ข้อมูล และทรัพยากรที่จำเป็น มีความพร้อม และสามารถนำมาใช้สนับสนุนการดำเนินธุรกิจได้ในกรณีเกิดเหตุการณ์หรืออุบัติการณ์ที่ทำให้เกิดภาวะวิกฤตหรือภัยคุกคามประเภทต่างๆ

3. คำจำกัดความ (Definition)

คำศัพท์ (Term)	คำอธิบาย (Description)
ความต่อเนื่องทางธุรกิจ (Business Continuity)	ความสามารถของบริษัทฯ ในการดำเนินงานอย่างต่อเนื่องในระดับที่บริษัทฯ ยอมรับได้ภายหลังเกิดเหตุการณ์ที่ทำให้การดำเนินงานหยุดชะงัก
การบริหารความต่อเนื่องทางธุรกิจ (Business Continuity Management: BCM)	กระบวนการบริหารแบบองค์รวมซึ่งระบุภัยคุกคามที่อาจเกิดขึ้นต่อบริษัทฯ และผลกระทบของภัยคุกคามดังกล่าวต่อการดำเนินธุรกิจ และกำหนดแนวทางในการเสริมสร้างความสามารถของบริษัทฯ ในการรับมือและฟื้นตัวจากเหตุการณ์ที่ทำให้การดำเนินงานหยุดชะงัก เพื่อปกป้องผลประโยชน์ของผู้มีส่วนได้เสียที่สำคัญ ชื่อเสียงและภาพลักษณ์ของบริษัทฯ ตลอดจนกิจกรรมที่สร้างคุณค่าให้แก่บริษัทฯ
ระบบการบริหารความต่อเนื่องทางธุรกิจ (Business Continuity Management System: BCMS)	ส่วนหนึ่งของระบบการบริหารซึ่งประกอบด้วยการวางแผน การจัดทำ การนำไปปฏิบัติ การดำเนินการ การติดตาม การทบทวน การรักษาและปรับปรุงให้เกิดความต่อเนื่องทางธุรกิจของบริษัทฯ ที่ใช้ในการกำหนด จัดทำ นำไปปฏิบัติ ดำเนินการ ติดตาม ทบทวน รักษา และปรับปรุงการบริหารความต่อเนื่องทางธุรกิจอย่างต่อเนื่อง
แผนความต่อเนื่องทางธุรกิจ (Business Continuity Plan: BCP)	ขั้นตอนที่เป็นลายลักษณ์อักษรสำหรับเป็นแนวทางให้บริษัทฯ ใช้ในการตอบสนอง กู้คืน ดำเนินงานอย่างต่อเนื่อง และฟื้นคืนการดำเนินงานไปยังระดับที่กำหนดไว้ล่วงหน้า เมื่อเกิดเหตุที่ทำให้การดำเนินงานหยุดชะงัก
ระยะเวลาเป้าหมายในการฟื้นคืนสภาพ (Recovery Time Objective: RTO)	ระยะเวลาเป้าหมายนับจากเวลาที่เกิดเหตุการณ์หรืออุบัติการณ์ที่ทำให้การดำเนินธุรกิจเกิดการหยุดชะงัก ซึ่งภายในระยะเวลาดังกล่าว การดำเนินกิจกรรม กระบวนการ หรือทรัพยากรที่เกี่ยวข้องจะต้องได้รับการฟื้นคืนให้อยู่ในระดับขั้นต่ำที่บริษัทฯ กำหนดและยอมรับได้
ช่วงเวลาการหยุดชะงักสูงสุดที่ยอมรับได้ (Maximum Tolerable Period of Disruption: MTPD)	ช่วงเวลาสูงสุดที่บริษัทฯ สามารถยอมรับให้การดำเนินกิจกรรมที่สำคัญหยุดชะงักได้ โดยหากเกินกว่าช่วงเวลาดังกล่าว อาจก่อให้เกิดผลกระทบในระดับที่บริษัทฯ ไม่อาจยอมรับได้
เป้าหมายของการฟื้นคืนสภาพ (Recovery Point Objective: RPO)	จุดเวลาเป้าหมายที่ข้อมูลสารสนเทศจะต้องได้รับการกู้คืนภายหลังเกิดเหตุการณ์หรืออุบัติการณ์ที่ทำให้การดำเนินธุรกิจเกิดการหยุดชะงัก ซึ่งใช้กำหนดปริมาณข้อมูลสารสนเทศสูงสุดที่บริษัทฯ ยอมรับให้สูญหายได้ โดยพิจารณาจากระยะเวลาระหว่างการสำรองข้อมูลครั้งล่าสุดกับเวลาที่เกิดเหตุการณ์หรืออุบัติการณ์
แผนกู้คืนระบบจากภัยพิบัติ (Disaster Recovery Plan: DRP)	แผนกู้คืนระบบที่บริษัทฯ จัดทำขึ้นเพื่อเตรียมความพร้อมในการกู้คืนระบบ ข้อมูล หรือโครงสร้างพื้นฐานด้านเทคโนโลยีสารสนเทศ หลังเกิดเหตุการณ์หรืออุบัติการณ์ที่ไม่คาดคิด เช่น ไฟไหม้ แผ่นดินไหว น้ำท่วม ระบบสารสนเทศล่ม หรือการโจมตีทางไซเบอร์ เพื่อให้ระบบและบริการด้านเทคโนโลยีสารสนเทศสามารถกลับมาใช้งานได้ภายในระยะเวลาและระดับที่กำหนด และเพื่อลดผลกระทบที่อาจเกิดขึ้น

คำศัพท์ (Term)	คำอธิบาย (Description)
แผนความต่อเนื่องทางธุรกิจด้านเทคโนโลยีสารสนเทศ (Information Technology Business Continuity Plan: IT BCP)	แผนความต่อเนื่องทางธุรกิจที่กำหนดแนวทาง บทบาท หน้าที่ และขั้นตอนเพื่อให้ระบบและบริการเทคโนโลยีสารสนเทศที่สำคัญ (Critical IT Services) สามารถดำเนินงานได้อย่างต่อเนื่อง โดยมีการหยุดชะงักน้อยที่สุด หรือได้รับการฟื้นคืนภายในระยะเวลาและระดับที่กำหนด ในระหว่างหรือภายหลังเกิดภาวะวิกฤต
การวิเคราะห์ผลกระทบทางธุรกิจ (Business Impact Analysis: BIA)	กระบวนการวิเคราะห์กิจกรรมและกระบวนการดำเนินงานของบริษัทฯ เพื่อประเมินผลกระทบที่อาจเกิดขึ้นจากการหยุดชะงัก ระบุลำดับความสำคัญในการฟื้นคืนการดำเนินงาน รวมถึงกำหนดระยะเวลาเป้าหมายและทรัพยากรที่จำเป็นสำหรับการฟื้นคืนกิจกรรมหรือการดำเนินงานที่สำคัญ
ภาวะวิกฤต (Crisis)	เหตุการณ์ อุบัติการณ์ หรือภัยพิบัติที่เกิดขึ้น ซึ่งอาจส่งผลให้การดำเนินธุรกิจหรือการให้บริการเกิดการหยุดชะงัก รวมถึงอาจกระทบต่อบุคลากร ทรัพย์สิน ระบบงาน ข้อมูล ชื่อเสียง ผู้มีส่วนได้เสีย หรือการบรรลุวัตถุประสงค์ขององค์กร
บุคลากร	พนักงาน ลูกจ้าง และผู้ให้บริการภายนอก

4. ขอบเขต (Scope)

บริษัทฯ กำหนดให้ทุกแผนกภายในบริษัทฯ เป็นส่วนหนึ่งของขอบเขตของระบบการบริหารความต่อเนื่องทางธุรกิจ (Business Continuity Management System: BCMS) โดยทุกแผนกต้องดำเนินการวิเคราะห์สภาพแวดล้อมและผลกระทบทางธุรกิจอย่างเป็นระบบ เพื่อระบุกิจกรรมและกระบวนการดำเนินงานที่สำคัญและกำหนดมาตรการรองรับเหตุการณ์ที่ทำให้เกิดภาวะวิกฤตหรือทำให้การดำเนินธุรกิจเกิดการหยุดชะงัก ทั้งนี้ บริษัทฯ จะระบุ ทบทวน และจัดกลุ่มกิจกรรมและกระบวนการที่เกี่ยวข้องกับการบริหารความต่อเนื่องทางธุรกิจ (Business Continuity Management : BCM) เป็นประจำ หรือเมื่อมีการเปลี่ยนแปลงที่มีนัยสำคัญ โดยพิจารณาจากผลการวิเคราะห์ผลกระทบทางธุรกิจ (Business Impact Analysis: BIA) และการประเมินความเสี่ยงที่เกี่ยวข้อง ทั้งนี้ กิจกรรมและกระบวนการที่อยู่ภายใต้ขอบเขตของระบบการบริหารความต่อเนื่องทางธุรกิจ (Business Continuity Management System: BCMS) ประจำปี 2569 มีดังต่อไปนี้

4.1 แผนกที่เกี่ยวข้อง

- BPA & Consolidation
- Corporate Finance & Accounting
- Treasury and Investor Relations
- Business Development
- Corporate Affairs
- Corporate Administration
- CEO Office and Support Team
- Corporate Communications
- Corporate Human Resources
- Information Technology

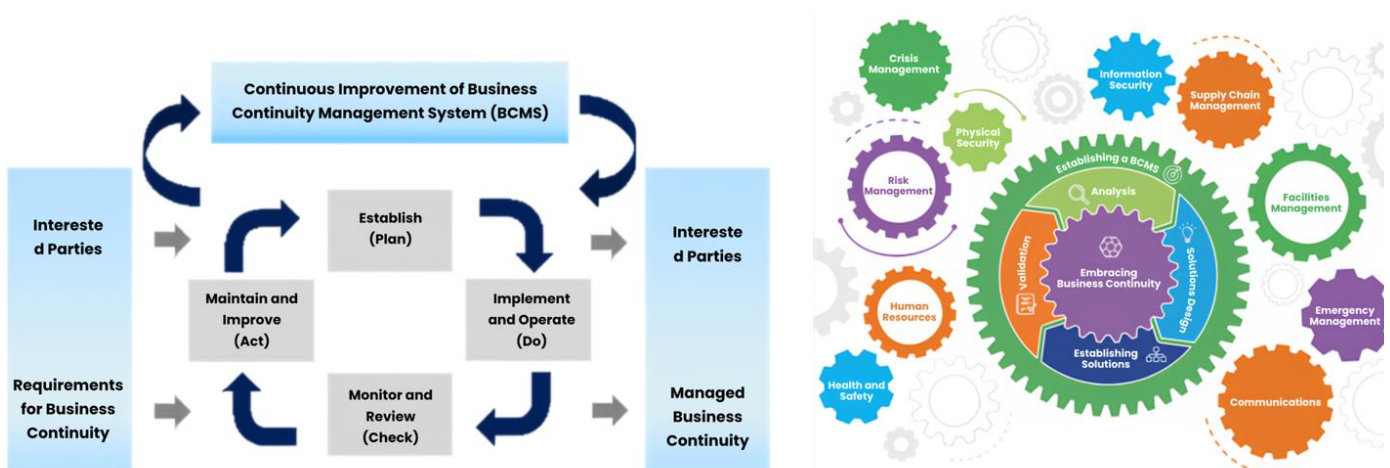
- Internal Audit, Compliance & Risk Management
- Corporate Legal

4.2 สถานที่ตั้ง

บริษัท โทริเซนไทย เอเยนซ์ซีส์ จำกัด (มหาชน) ตั้งอยู่เลขที่ 26/26-27 อาคารอรกานต์ ชั้น 8 ซอยชิดลม ถนนเพลินจิต แขวงลุมพินี เขตปทุมวัน กรุงเทพมหานคร 10330

5. กรอบการบริหารความต่อเนื่องทางธุรกิจ (Business Continuity Framework)

บริษัทฯ ได้นำวงจรการบริหารแบบ Plan-Do-Check-Act (PDCA) และวงจรการบริหารความต่อเนื่องทางธุรกิจ (BCM Lifecycle) ตามมาตรฐานสากลและแนวปฏิบัติที่ดี (Good Practice Guidelines: GPG) มาประยุกต์ใช้ในการพัฒนาระบบการบริหารความต่อเนื่องทางธุรกิจ (Business Continuity Management System: BCMS) โดยประกอบด้วยขั้นตอนหลัก ดังนี้



รูปที่ 1 PDCA Model และ BCM Lifecycle

นโยบายการบริหารความต่อเนื่องทางธุรกิจ

แผนบริหารความเสี่ยง

วันที่มีผลบังคับใช้

ฉบับที่ 1, แก้ไขครั้งที่ 00

11 สิงหาคม 2569

PDCA	รายละเอียด	BCM Lifecycle
Plan (วางแผน)	กำหนดนโยบายการบริหารความต่อเนื่องทางธุรกิจ (Business Continuity Management Policy: BCMP) วัตถุประสงค์ เป้าหมาย การควบคุม กระบวนการ และขั้นตอนที่เกี่ยวข้องกับการพัฒนาความต่อเนื่องทางธุรกิจซึ่งสอดคล้องกับนโยบายและวัตถุประสงค์โดยรวมของบริษัทฯ	- การจัดตั้งระบบการบริหารความต่อเนื่องทางธุรกิจ (Business Continuity Management System: BCMS) - การปลูกฝังวัฒนธรรมความต่อเนื่องทางธุรกิจในองค์กร
Do (ปฏิบัติ)	นำนโยบายการบริหารความต่อเนื่องทางธุรกิจ (Business Continuity Management Policy: BCMP) การควบคุม กระบวนการ และขั้นตอนที่เกี่ยวข้องไปปฏิบัติ	- การวิเคราะห์ - การออกแบบแนวทางแก้ไขปัญหา - การประยุกต์ใช้แนวทางแก้ไขปัญหา - การตรวจสอบความถูกต้อง
Check (ตรวจสอบ)	ตรวจสอบ และทบทวนผลการดำเนินงานตามนโยบาย และ วัตถุประสงค์ความต่อเนื่องทางธุรกิจ (Business Continuity) รวมถึงรายงานผลการดำเนินงานต่อผู้บริหาร เพื่อพิจารณาความ มีประสิทธิภาพของระบบและกำหนดแนวทางในการแก้ไขหรือ ปรับปรุงตามความเหมาะสม	- การประเมินผลการดำเนินงาน - การตรวจสอบภายใน - การทบทวนโดยฝ่ายบริหาร
Act (ดำเนินการ)	รักษา และปรับปรุงระบบการบริหารความต่อเนื่องทางธุรกิจ (Business Continuity Management System: BCMS) โดย ดำเนินการแก้ไขและปรับปรุงตามผลการติดตาม การตรวจสอบ และการทบทวนโดยฝ่ายบริหาร รวมถึงทบทวนขอบเขตของ ระบบการบริหารความต่อเนื่องทางธุรกิจ (Business Continuity Management System: BCMS) นโยบาย และวัตถุประสงค์ ความต่อเนื่องทางธุรกิจ (Business Continuity) เพื่อให้มีความ เหมาะสมและมีประสิทธิภาพอย่างต่อเนื่อง	การปรับปรุงแก้ไข

นโยบายการบริหารความต่อเนื่องทางธุรกิจ

แผนกบริหารความเสี่ยง

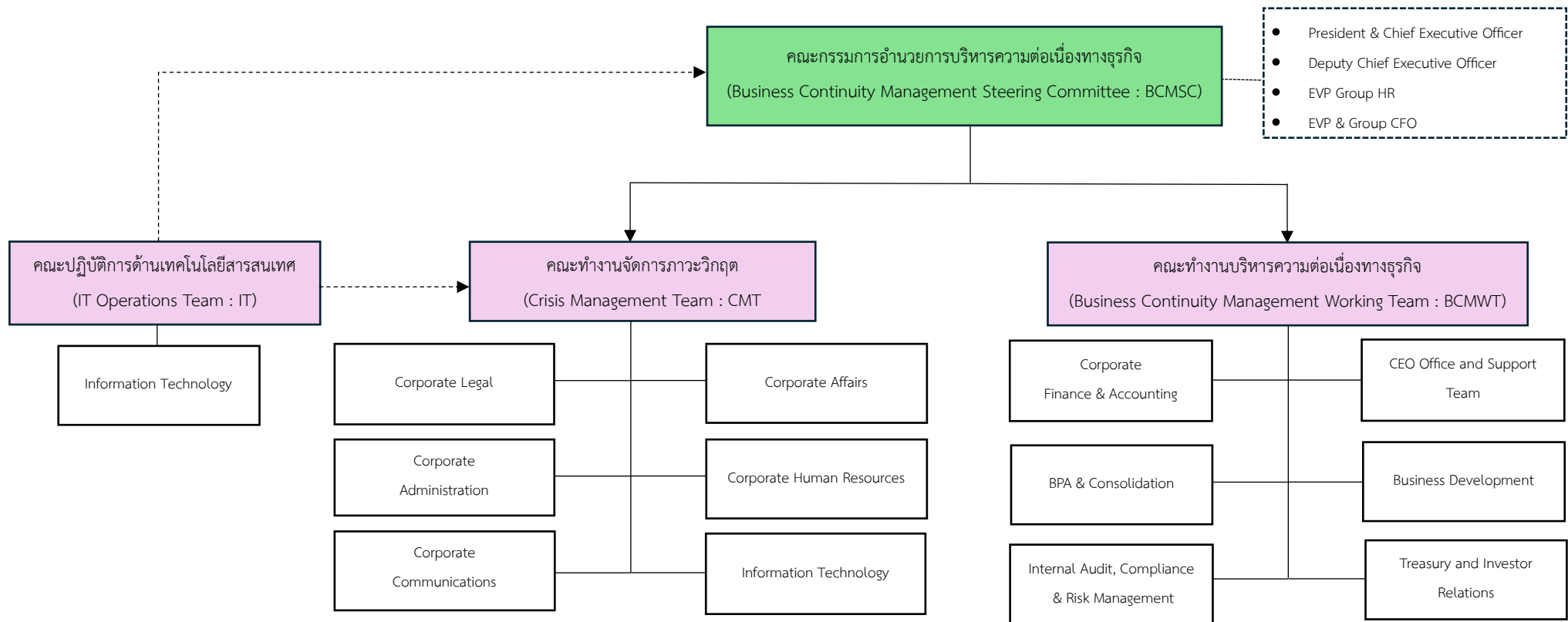
วันที่มีผลบังคับใช้

ฉบับที่ 1, แก้ไขครั้งที่ 00

11 สิงหาคม 2569

6. บทบาท และความรับผิดชอบ (Roles and Responsibilities)

6.1 โครงสร้างการกำกับดูแลการบริหารความต่อเนื่องทางธุรกิจ



นโยบายการบริหารความต่อเนื่องทางธุรกิจ

แผนกบริหารความเสี่ยง

วันที่มีผลบังคับใช้

ฉบับที่ 1, แก้ไขครั้งที่ 00

11 สิงหาคม 2569

6.2 บทบาท หน้าที่ และความรับผิดชอบ

6.2.1 คณะกรรมการอำนวยการบริหารความต่อเนื่องทางธุรกิจ (Business Continuity Management Steering Committee: BCMSC)

1) ในภาวะปกติ

- กำกับดูแลเพื่อให้กระบวนการบริหารความต่อเนื่องทางธุรกิจ (Business Continuity Management: BCM) ของทุกแผนกภายในบริษัทฯ ให้เป็นไปอย่างมีประสิทธิภาพ
- กำหนดนโยบายการดำเนินงานด้านระบบการบริหารความต่อเนื่องทางธุรกิจ (Business Continuity Management System: BCMS) ของบริษัทฯ โดยใช้มาตรฐาน ISO 22301 เป็นแนวทางในการดำเนินงาน
- อนุมัติและทบทวนระบบการบริหารความต่อเนื่องทางธุรกิจ (Business Continuity Management System: BCMS) ของบริษัทฯ รวมถึงแนวทางในการพัฒนาและปรับปรุงระบบดังกล่าวให้ทันสมัยและสอดคล้องกับสถานการณ์ที่เปลี่ยนแปลงอยู่เสมอ
- สนับสนุน ช่วยเหลือ และให้ข้อเสนอแนะต่อการพัฒนาระบบการบริหารความต่อเนื่องทางธุรกิจ (Business Continuity Management System: BCMS) และการเตรียมความพร้อมรองรับกับภาวะวิกฤตที่อาจส่งผลให้การดำเนินงานของบริษัทฯ หยุดชะงัก
- พิจารณา และอนุมัติงบประมาณ เพื่อสนับสนุนการดำเนินการที่เกี่ยวกับการบริหารความต่อเนื่องทางธุรกิจ (Business Continuity Management: BCM) ของบริษัทฯ ให้บรรลุวัตถุประสงค์

2) ในภาวะวิกฤต

- พิจารณาและสั่งการเกี่ยวกับการประกาศใช้ การดำเนินการตาม และการยกเลิกการใช้แผนความต่อเนื่องทางธุรกิจ (Business Continuity Plan: BCP)
- President & Chief Executive Officer มีอำนาจตัดสินใจประกาศใช้และยกเลิกการใช้แผนความต่อเนื่องทางธุรกิจ (Business Continuity Plan: BCP) ของบริษัทฯ ในกรณีที่ President & Chief Executive Officer ไม่สามารถปฏิบัติหน้าที่ได้ ให้ Deputy Chief Executive Officer มีอำนาจตัดสินใจดังกล่าวแทน เว้นแต่บริษัทฯ จะกำหนดผู้มีอำนาจอื่นไว้เป็นลายลักษณ์อักษร
- พิจารณาสถานการณ์ วางกลยุทธ์ และออกคำสั่งเพิ่มเติม ในกรณีที่เกิดเหตุการณ์หรืออุบัติการณ์ที่ไม่คาดคิด หรือมีสถานการณ์แตกต่างจากที่กำหนดไว้ในแผนความต่อเนื่องทางธุรกิจ (Business Continuity Plan: BCP)
- ติดตามและกำกับดูแลการดำเนินการตามแผนความต่อเนื่องทางธุรกิจ (Business Continuity Plan: BCP) ขณะเกิดเหตุการณ์หรืออุบัติการณ์ เพื่อให้สามารถควบคุมหรือบรรเทาผลกระทบจากสถานการณ์ได้โดยเร็ว และเพื่อให้การดำเนินงานที่สำคัญของบริษัทฯ สามารถดำเนินการได้อย่างต่อเนื่องหรือได้รับการฟื้นคืนภายในระยะเวลาและระดับที่กำหนด

นโยบายการบริหารความต่อเนื่องทางธุรกิจ

แผนกบริหารความเสี่ยง

วันที่มีผลบังคับใช้

ฉบับที่ 1, แก้ไขครั้งที่ 00

11 สิงหาคม 2569

3) ในภาวะหลังวิกฤต

- อำนาจการฟื้นฟูปรับปรุงสำนักงาน เพื่อให้สามารถใช้เป็นสถานที่ปฏิบัติงานได้ตามปกติ
- อนุมัติแผนการฟื้นฟูสำนักงานเพื่อให้สามารถใช้เป็นสถานที่ปฏิบัติงานได้ตามปกติ
- กำกับดูแลการฟื้นคืนกระบวนการดำเนินงาน ระบบเทคโนโลยีสารสนเทศ บุคลากร และทรัพยากรที่สำคัญของบริษัทฯ ให้กลับสู่ภาวะปกติหรือระดับที่บริษัทฯ กำหนดว่ายอมรับได้
- กำกับให้มีการทบทวนผลการตอบสนองต่อเหตุการณ์หรืออุบัติการณ์ สาเหตุของการหยุดชะงัก ปัญหาและข้อบกพร่องที่พบ ตลอดจนกำหนดมาตรการแก้ไขและปรับปรุงแผนความต่อเนื่องทางธุรกิจ (Business Continuity Plan: BCP) เพื่อป้องกันการเกิดเหตุซ้ำ

6.2.2 คณะทำงานจัดการภาวะวิกฤต (Crisis Management Team: CMT)

1) ในภาวะปกติ

- พิจารณา ทบทวนภัยคุกคามประจำปี ทั้งด้านกายภาพและด้านความมั่นคงปลอดภัยไซเบอร์ รวมถึงทบทวนและปรับปรุงการวิเคราะห์ผลกระทบทางธุรกิจ และการประเมินความเสี่ยง ให้ครอบคลุมความเสี่ยงจากภัยคุกคามด้านไซเบอร์ เช่น Ransomware, Cyberattack, Data Breach, Malware, Phishing และการหยุดชะงักของระบบเทคโนโลยีสารสนเทศ
- จัดให้มีการฝึกซ้อมและทดสอบแผนอพยพบุคลากรของบริษัทฯ กรณีเกิดเหตุการณ์หรืออุบัติการณ์ที่ส่งผลให้สำนักงานไม่สามารถใช้ปฏิบัติงานได้ตามปกติ รวมถึงทบทวนและทดสอบแผนรับมือเหตุการณ์ด้านความมั่นคงปลอดภัยไซเบอร์ โดยร่วมกับแผนก Information Technology และแผนกที่เกี่ยวข้อง ซึ่งอาจดำเนินการในรูปแบบการฝึกซ้อมบนโต๊ะ (Tabletop Exercise) อย่างน้อยปีละหนึ่ง (1) ครั้ง
- ควบคุม กำกับดูแล ให้การป้องกัน และบรรเทาสาธารณภัย รวมถึงการป้องกันภัยคุกคามด้านเทคโนโลยีสารสนเทศและความมั่นคงปลอดภัยไซเบอร์ให้เป็นไปอย่างมีประสิทธิภาพและประสิทธิผล
- ติดตามและประเมินสถานการณ์ที่อาจเกิดขึ้น วางระบบเตือนภัย และกำหนดมาตรการต่างๆ ในการปฏิบัติการกู้ชีพ กู้ภัย อพยพ ช่วยเหลือผู้ที่ได้รับบาดเจ็บ และการตอบสนองต่อเหตุการณ์ด้านไซเบอร์
- ประสานงานร่วมกับแผนก Information Technology และหน่วยงานที่เกี่ยวข้อง ในการเฝ้าระวัง ตรวจสอบ วิเคราะห์ และตอบสนองต่อเหตุการณ์ผิดปกติด้านความมั่นคงปลอดภัยไซเบอร์ รวมถึงกำกับดูแลให้มีการสำรองข้อมูลและการทดสอบความสามารถในการกู้คืนข้อมูลตามระยะเวลาที่กำหนด

2) ในภาวะวิกฤต

- ประสานงานขอความช่วยเหลือกับหน่วยงานภายนอก เช่น สถานีดับเพลิง สถานีตำรวจ โรงพยาบาล ผู้ให้บริการระบบเทคโนโลยีสารสนเทศ ผู้ให้บริการ Cloud / Data Center และหน่วยงานกำกับดูแลที่เกี่ยวข้อง เป็นต้น
- ตรวจสอบ ประเมินความเสียหายเบื้องต้นของสำนักงาน ระบบเทคโนโลยีสารสนเทศ ระบบเครือข่าย ฐานข้อมูล และทรัพย์สินสารสนเทศ เมื่อเกิดภาวะวิกฤตที่กระทบต่อสำนักงาน หรือเกิดเหตุการณ์ด้านความ

นโยบายการบริหารความต่อเนื่องทางธุรกิจ

แผนกบริหารความเสี่ยง

วันที่มีผลบังคับใช้

ฉบับที่ 1, แก้ไขครั้งที่ 00

11 สิงหาคม 2569

มั่นคงปลอดภัยไซเบอร์ เช่น Cyberattack, Ransomware, Malware, Phishing, Data Breach, ระบบถูกบุกรุก หรือการรั่วไหลของข้อมูลสำคัญ และการหยุดชะงักของระบบเทคโนโลยีสารสนเทศ

- ประเมินความรุนแรงของสถานการณ์ ผลกระทบต่อบริษัท ความเสียหายต่อบุคลากร กระบวนการที่สำคัญ สถานที่ปฏิบัติงานหลัก สิ่งอำนวยความสะดวก ระบบเทคโนโลยีสารสนเทศ ขอบเขตความเสียหาย และระดับความรุนแรงของอุบัติการณ์ที่เกิดขึ้น รวมถึงเหตุการณ์ด้านความมั่นคงปลอดภัยไซเบอร์ เช่น Cyberattack, Ransomware, Malware, Phishing หรือ Data Breach และการหยุดชะงักของระบบเทคโนโลยีสารสนเทศ และรายงานต่อคณะกรรมการอำนวยการบริหารความต่อเนื่องทางธุรกิจ (Business Continuity Management Steering Committee: BCMSC)
- รายงานผลการประเมินความเสียหายพร้อมข้อเสนอแนะและแนวทางดำเนินการเสนอต่อคณะกรรมการอำนวยการบริหารความต่อเนื่องทางธุรกิจ (Business Continuity Management Steering Committee: BCMSC) เพื่อประกอบการพิจารณาประกาศใช้แผนความต่อเนื่องทางธุรกิจ (Business Continuity Plan: BCP)
- อพยพพนักงานไปที่จุดรวมพล ให้ความช่วยเหลือเบื้องต้นแก่ผู้ได้รับบาดเจ็บ และประสานงานเพื่อนำส่งผู้ได้รับบาดเจ็บหรือผู้ป่วยไปรับการรักษาโดยเร็ว
- สั่งการ ควบคุม และติดตามความคืบหน้าของกิจกรรมการกู้คืน และรายงานต่อคณะกรรมการอำนวยการบริหารความต่อเนื่องทางธุรกิจ (Business Continuity Management Steering Committee: BCMSC) ให้ทราบเป็นระยะ
- ติดตามสถานการณ์ จนกว่าภาวะวิกฤตหรืออุบัติการณ์ จะได้รับการควบคุมหรือคลี่คลาย และแจ้งข่าวสารความคืบหน้าให้แก่พนักงานและบุคลากรของบริษัทฯ ตามช่องทางและหลักเกณฑ์การสื่อสารที่บริษัทฯ กำหนด
- จัดทำและเก็บรักษาบันทึกเหตุการณ์ การตัดสินใจ คำสั่ง และการดำเนินการที่เกี่ยวข้อง (Incident Log) รวมถึงรายงานความคืบหน้าต่อคณะกรรมการอำนวยการบริหารความต่อเนื่องทางธุรกิจ (Business Continuity Management Steering Committee: BCMSC)
- กรณีเกิด Ransomware / Data Breach ให้แผนก Information Technology ดำเนินการควบคุมเหตุ ประเมินขอบเขตและผลกระทบเบื้องต้น และรายงานเหตุการณ์ต่อคณะทำงานจัดการภาวะวิกฤต (Crisis Management Team: CMT) โดยทันทีและไม่เกินหนึ่ง (1) ชั่วโมงนับแต่ทราบเหตุ โดยคณะทำงานจัดการภาวะวิกฤต (Crisis Management Team: CMT) จะประสานแผนก Information Technology แผนก Corporate Legal และแผนก Corporate Communications เพื่อดำเนินการตามระดับความรุนแรงของเหตุการณ์ (Incident Severity Levels) (P1-P4) และประสานเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (Data Protection Officer: DPO) ทันที เมื่อเกิดหรือสงสัยว่าจะเกิดเหตุละเมิดข้อมูลส่วนบุคคล (Personal Data Breach) รวมถึงการสูญหาย การเข้าถึง การใช้ การเปลี่ยนแปลง แก้ไข หรือเปิดเผยข้อมูลส่วนบุคคลโดยปราศจากอำนาจหรือโดยมิชอบ ทั้งนี้ ให้แผนก Corporate Legal เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (Data Protection Officer: DPO) และแผนกที่เกี่ยวข้องร่วมกันประเมินลักษณะ ขอบเขต และระดับ

นโยบายการบริหารความต่อเนื่องทางธุรกิจ

แผนกบริหารความเสี่ยง

วันที่มีผลบังคับใช้

ฉบับที่ 1, แก้ไขครั้งที่ 00

11 สิงหาคม 2569

ความเสี่ยงของเหตุการณ์ และดำเนินการให้บริษัทฯ แจ้งเหตุละเมิดต่อสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลโดยไม่ชักช้า และเท่าที่สามารถกระทำได้ภายในเจ็ดสิบสอง (72) ชั่วโมงนับแต่บริษัทฯ ทราบเหตุ เว้นแต่เหตุละเมิดดังกล่าวไม่มีแนวโน้มที่จะก่อให้เกิดความเสี่ยงต่อสิทธิและเสรีภาพของบุคคล ตลอดจนแจ้งเหตุและมาตรการเยียวยาแก่เจ้าของข้อมูลส่วนบุคคลโดยไม่ชักช้า ในกรณีที่เหตุละเมิดนั้น มีความเสี่ยงสูงต่อสิทธิและเสรีภาพของบุคคล ทั้งนี้ ให้เป็นไปตามกฎหมายและหลักเกณฑ์ที่เกี่ยวข้อง

3) ในภาวะหลังวิกฤต

- ตรวจสอบ ประเมินความเสียหายของอาคารสำนักงานรวมถึงระบบเทคโนโลยีสารสนเทศ ระบบเครือข่าย ฐานข้อมูล และทรัพย์สินสารสนเทศ ภายหลังเกิดภาวะวิกฤต หรือเหตุการณ์ด้านความมั่นคงปลอดภัยไซเบอร์
- ประสานงานและกำกับดูแลการบูรณะหรือซ่อมแซมอาคารสำนักงานที่ได้รับความเสียหายให้กลับคืนสู่สภาพที่ปลอดภัยและสามารถใช้งานได้ตามปกติหรือในระดับที่บริษัทฯ ยอมรับได้ รวมถึงกู้คืนระบบเทคโนโลยีสารสนเทศ ระบบงานที่สำคัญ และข้อมูลสารสนเทศสามารถกลับมาใช้งานได้ในระยะเวลาและระดับที่กำหนด พร้อมทั้งตรวจสอบความถูกต้อง ความครบถ้วน ความสมบูรณ์ ตลอดจนความมั่นคงปลอดภัยของระบบและข้อมูลภายหลังการกู้คืน
- รายงานผลการประเมินความพร้อมใช้งานของอาคารสำนักงานและระบบเทคโนโลยีสารสนเทศ รวมถึงความพร้อมของบุคลากร กระบวนการดำเนินงาน และทรัพยากรที่สำคัญต่อคณะกรรมการอำนวยการบริหารความต่อเนื่องทางธุรกิจ (Business Continuity Management Steering Committee: BCMSC) ประกอบการพิจารณาประกาศยกเลิกการใช้แผนความต่อเนื่องทางธุรกิจ (Business Continuity Plan: BCP)
- จัดทำบทเรียนจากเหตุการณ์ (Lessons Learned) ทบทวน และปรับปรุงแผนรับมือเหตุการณ์ด้านไซเบอร์ และมาตรการควบคุมด้านความมั่นคงปลอดภัยไซเบอร์ ให้มีความเหมาะสมและสอดคล้องกับความเสี่ยงที่เกิดขึ้น รวมถึงติดตามการดำเนินการแก้ไขข้อบกพร่องที่ตรวจพบจนแล้วเสร็จ

6.2.3 คณะทำงานบริหารความต่อเนื่องทางธุรกิจ (Business Continuity Management Working Team: BCMWT)

1) ในภาวะปกติ

- จัดทำ กำกับ และทบทวนกระบวนการบริหารความต่อเนื่องทางธุรกิจ (Business Continuity Management: BCM) ให้เป็นปัจจุบันและสอดคล้องกับสถานการณ์ที่เปลี่ยนแปลงอยู่เสมอ โดยสามารถจัดประชุมกลุ่มย่อยได้ตามความเหมาะสม เพื่อเสนอผลการดำเนินงานและข้อเสนอแนะต่อคณะกรรมการอำนวยการบริหารความต่อเนื่องทางธุรกิจ (Business Continuity Management Steering Committee: BCMSC) เพื่อพิจารณาให้ความเห็นชอบ
- สนับสนุนการจัดทำ นำไปปฏิบัติ ทบทวนและปรับปรุงระบบการบริหารความต่อเนื่องทางธุรกิจ (Business Continuity Management System: BCMS) ของบริษัทฯ
- กำกับดูแลให้มีการทดสอบและฝึกซ้อมแผนความต่อเนื่องทางธุรกิจ (Business Continuity Plan: BCP) ของหน่วยงาน พร้อมทั้งรายงานผลการฝึกซ้อมและปัญหาอุปสรรคให้แก่คณะกรรมการอำนวยการบริหาร

นโยบายการบริหารความต่อเนื่องทางธุรกิจ

แผนบริหารความเสี่ยง

วันที่มีผลบังคับใช้

ฉบับที่ 1, แก้ไขครั้งที่ 00

11 สิงหาคม 2569

ความต่อเนื่องทางธุรกิจ (Business Continuity Management Steering Committee: BCMSC) รับทราบ และกำกับติดตามการแก้ไขข้อบกพร่องที่ตรวจพบ

- สื่อสารแผนความต่อเนื่องทางธุรกิจ (Business Continuity Plan: BCP) ของบริษัทฯ ให้พนักงานและบุคลากรในหน่วยงานตามสายการบังคับบัญชารับทราบ ตระหนักถึงความสำคัญ และยึดถือปฏิบัติเป็นแนวทางเดียวกัน
- ประชาสัมพันธ์ และส่งเสริมให้พนักงานและบุคลากรทั้งหมดในบริษัทฯ ได้รับความรู้ ความเข้าใจ และเกิดความตระหนักเกี่ยวกับการบริหารความต่อเนื่องทางธุรกิจ (Business Continuity Management: BCM)
- ประสานงานกับหน่วยงานที่เกี่ยวข้องในการจัดทำและทบทวนการวิเคราะห์ผลกระทบทางธุรกิจ (Business Impact Analysis: BIA) การประเมินความเสี่ยง และแผนความต่อเนื่องทางธุรกิจของแต่ละแผนกให้เป็นปัจจุบัน

2) ในภาวะวิกฤต

- นำคำสั่งประกาศใช้แผนความต่อเนื่องทางธุรกิจ (Business Continuity Plan: BCP) และแนวทางปฏิบัติจากคณะกรรมการอำนวยการบริหารความต่อเนื่องทางธุรกิจ (Business Continuity Management Steering Committee: BCMSC) ไปถ่ายทอดและสื่อสารให้แก่พนักงานและบุคลากรในหน่วยงานตามสายการบังคับบัญชาของตนทราบและปฏิบัติตามอย่างถูกต้องและทันต่อสถานการณ์
- มอบหมายงานตามบทบาท หน้าที่ และความรับผิดชอบแก่บุคลากรภายใต้สายการบังคับบัญชาและกำกับติดตามให้มีการปฏิบัติตามแผนและคำสั่งที่เกี่ยวข้อง
- สนับสนุนอุปกรณ์การปฏิบัติงานและอุปกรณ์ด้านเทคโนโลยีสารสนเทศเพื่ออำนวยความสะดวกแก่ผู้ที่เกี่ยวข้อง เมื่อมีการปฏิบัติงาน ณ ที่พักอาศัย
- ติดตามความคืบหน้าในการประสานงานและรายงานผลการปฏิบัติงานตามรูปแบบและสถานที่ปฏิบัติงานที่บริษัทฯ กำหนดในภาวะวิกฤต
- ประสานงานกับหน่วยงานที่เกี่ยวข้องเพื่อให้กระบวนการดำเนินงานที่สำคัญสามารถดำเนินต่อไปหรือได้รับการฟื้นคืนภายในระยะเวลาและระดับที่กำหนด

3) ในภาวะหลังวิกฤต

- จัดทำแผนฟื้นฟูของบริษัทฯ ร่วมกับแผนกที่เกี่ยวข้อง เพื่อนำเสนอต่อคณะกรรมการอำนวยการบริหารความต่อเนื่องทางธุรกิจ (Business Continuity Management Steering Committee: BCMSC) พิจารณาให้ความเห็นชอบ
- ดำเนินการตามแผนฟื้นฟูที่คณะกรรมการอำนวยการบริหารความต่อเนื่องทางธุรกิจ (Business Continuity Management Steering Committee: BCMSC) ได้ให้ความเห็นชอบแล้ว และรายงานความคืบหน้าตามระยะเวลาที่กำหนด

นโยบายการบริหารความต่อเนื่องทางธุรกิจ

แผนกบริหารความเสี่ยง

วันที่มีผลบังคับใช้

ฉบับที่ 1, แก้ไขครั้งที่ 00

11 สิงหาคม 2569

- ติดตามความคืบหน้าในการประสานงานและรายงานผลการกลับเข้าปฏิบัติงาน ณ สถานที่ปฏิบัติงานหลัก หรือการกลับสู่การดำเนินงานตามปกติ พร้อมทั้งรวบรวมปัญหาอุปสรรคเสนอต่อคณะกรรมการอำนวยการบริหารความต่อเนื่องทางธุรกิจ (Business Continuity Management Steering Committee: BCMSC) เพื่อทราบ
- รวบรวมผลการดำเนินงาน ข้อบกพร่อง และบทเรียนที่ได้รับจากเหตุการณ์ เพื่อเสนอแนวทางแก้ไขและปรับปรุงผลการประเมินความเสี่ยง (Risk Assessment: RA) แผนความต่อเนื่องทางธุรกิจ (Business Continuity Plan: BCP) และมาตรการที่เกี่ยวข้องให้เหมาะสม

6.2.4 คณะปฏิบัติการด้านเทคโนโลยีสารสนเทศ (IT Operations Team: IT)

1) ในภาวะปกติ

- เข้าร่วมการทดสอบแผนความต่อเนื่องทางธุรกิจ (Business Continuity Plan: BCP) ของบริษัทฯ
- จัดทำ ทบทวน และปรับปรุงแผนกู้คืนระบบเทคโนโลยีสารสนเทศ รวมถึงกำกับดูแลให้แผนความต่อเนื่องทางธุรกิจ (Business Continuity Plan: BCP) และแผนกู้คืนระบบจากภัยพิบัติ (Disaster Recovery Plan: DRP) มีความสอดคล้องกันอยู่เสมอ
- ดำเนินการตรวจสอบความพร้อมของ Hardware / Software และอุปกรณ์ที่ใช้ในการปฏิบัติงานของระบบต่างๆ เพื่อสนับสนุนการปฏิบัติงานจากสถานที่ปฏิบัติงานสำรอง ที่พักอาศัย หรือสถานที่อื่นที่บริษัทฯ กำหนดอย่างสม่ำเสมอ
- ดูแลและทดสอบแผนความต่อเนื่องทางธุรกิจด้านเทคโนโลยีสารสนเทศและแผนกู้คืนระบบจากภัยพิบัติ (BCP-ITS-001) อย่างน้อยปีละหนึ่ง (1) ครั้ง และตรวจสอบว่าผลการทดสอบเป็นไปตามระยะเวลาเป้าหมายในการฟื้นคืนสภาพ (Recovery Time Objective: RTO) ตามการวิเคราะห์ผลกระทบทางธุรกิจ (Business Impact Analysis: BIA) รวมถึงประสานงานกับผู้รับผิดชอบของแต่ละแผนก เพื่อยืนยันลำดับความสำคัญของระบบและความต้องการในการกู้คืน
- ตรวจสอบและทดสอบการสำรองข้อมูล ความสามารถในการกู้คืนข้อมูล และความพร้อมของระบบสำรองโครงสร้างพื้นฐาน ผู้ให้บริการ และทรัพยากรที่จำเป็นตามรอบระยะเวลาที่บริษัทฯ กำหนด

2) ในภาวะวิกฤต

- จัดเตรียม Hardware / Software และอุปกรณ์ที่ใช้ในการปฏิบัติงานของระบบต่างๆ ที่จำเป็นเพื่อสนับสนุนการปฏิบัติงานจากสถานที่ปฏิบัติงานสำรอง ที่พักอาศัย หรือสถานที่อื่นที่บริษัทฯ กำหนด
- พิจารณาถึงลำดับความสำคัญของระบบงาน เพื่อเปิดใช้ ปิดใช้ ระบุ หรือจำกัดการใช้งานแต่ละระบบตามความจำเป็น โดยให้ความสำคัญกับระบบงานที่รองรับกระบวนการทางธุรกิจที่สำคัญก่อน และให้เป็นไปตามลำดับความสำคัญของระยะเวลาเป้าหมายในการฟื้นคืนสภาพ (Recovery Time Objective: RTO) และเป้าหมายของการฟื้นคืนสภาพ (Recovery Point Objective: RPO) ที่กำหนดไว้

นโยบายการบริหารความต่อเนื่องทางธุรกิจ

แผนกบริหารความเสี่ยง

วันที่มีผลบังคับใช้

ฉบับที่ 1, แก้ไขครั้งที่ 00

11 สิงหาคม 2569

- จัดเตรียมบุคลากรด้านเทคโนโลยีสารสนเทศให้เพียงพอต่อการกู้คืนระบบงานและการดำเนินการในระหว่างเกิดภาวะวิกฤตหรืออุบัติการณ์
- จัดเตรียมช่องทางการสื่อสารที่จำเป็นต่อการประสานงานและการกู้คืนระบบ ทั้งนี้ การสื่อสารกับผู้มีส่วนได้เสียภายนอกให้ดำเนินการร่วมกับแผนก Corporate Communications แผนก Corporate Legal และแผนกที่เกี่ยวข้องตามอำนาจหน้าที่
- จัดเตรียมช่องทางการสื่อสารในกรณีที่พนักงานหรือบุคลากรบางส่วนต้องปฏิบัติงานจากภายนอกสถานที่ปฏิบัติงานหลัก รวมถึงการปฏิบัติงาน ณ สถานที่ปฏิบัติงานสำรอง ที่พักอาศัย หรือสถานที่อื่นที่บริษัทฯ กำหนด
- จัดทำและเก็บรักษาบันทึกเหตุการณ์ การตัดสินใจ การเปลี่ยนแปลงระบบ และการดำเนินการที่เกี่ยวข้อง (Incident Log) รวมถึงรายงานความคืบหน้าต่อคณะกรรมการจัดการภาวะวิกฤต (Crisis Management Team: CMT) และคณะกรรมการอำนวยการบริหารความต่อเนื่องทางธุรกิจ (Business Continuity Management Steering Committee: BCMSC) ตามลำดับการรายงานและความเร่งด่วนของสถานการณ์
- ในกรณีเหตุการณ์ระดับ P1-P2 ให้หัวหน้าคณะปฏิบัติการด้านเทคโนโลยีสารสนเทศ (IT Operations Team: IT) มีอำนาจประกาศใช้แผนกู้คืนระบบจากภัยพิบัติ (Disaster Recovery Plan: DRP) และจัดตั้งศูนย์ประสานงานเหตุการณ์ (War Room) ได้ทันทีตามหลักเกณฑ์และขอบเขตอำนาจที่บริษัทฯ กำหนด โดยต้องรายงานต่อผู้บริหารที่รับผิดชอบและคณะกรรมการจัดการภาวะวิกฤต (Crisis Management Team: CMT) โดยทันที พร้อมแจ้งระยะเวลาโดยประมาณในการกู้คืน (Estimated Time to Recovery) และสถานะของระบบภายในหนึ่ง (1) ชั่วโมงนับแต่ประกาศใช้แผนกู้คืนระบบจากภัยพิบัติ (Disaster Recovery Plan: DRP) ทั้งนี้ หากเหตุการณ์ดังกล่าวเกี่ยวข้องหรืออาจเกี่ยวข้องกับเหตุละเมิดข้อมูลส่วนบุคคล ให้ประสานเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (Data Protection Officer: DPO) แผนก Corporate Legal และแผนกที่เกี่ยวข้องโดยทันที เพื่อประเมินและดำเนินการตามกฎหมายและหลักเกณฑ์ที่เกี่ยวข้อง
- ดำเนินการควบคุม แยกกัก กู้คืน และตรวจสอบระบบตามขั้นตอนที่กำหนด โดยคำนึงถึงการรักษาพยานหลักฐานดิจิทัล ความมั่นคงปลอดภัยของระบบ และการป้องกันมิให้เหตุการณ์ขยายวงกว้าง

3) ในภาวะหลังวิกฤต

- ประเมินความเสียหายของอุปกรณ์และระบบเทคโนโลยีสารสนเทศเมื่อเหตุการณ์ที่ทำให้เกิดภาวะวิกฤตหรืออุบัติการณ์เริ่มสงบหรือกลับเข้าสู่สภาวะปกติ
- สนับสนุนการดำเนินการฟื้นฟูระบบเทคโนโลยีสารสนเทศ รวมถึงตรวจสอบความถูกต้อง ความครบถ้วน ความสมบูรณ์ ตลอดจนความมั่นคงปลอดภัยของระบบและข้อมูลภายหลังการกู้คืน ก่อนนำระบบกลับมาใช้งาน
- จัดทำรายงานสรุปผลภายหลังเหตุการณ์ (Post-Incident Report) ภายในระยะเวลาที่เหมาะสมตามระดับความรุนแรงของเหตุการณ์ แต่ไม่เกินสี่ (4) สัปดาห์นับแต่เหตุการณ์ได้รับการควบคุมหรือคลี่คลาย เว้นแต่มีเหตุจำเป็นซึ่งต้องได้รับความเห็นชอบจากผู้บริหารที่รับผิดชอบ และเสนอต่อคณะกรรมการ

นโยบายการบริหารความต่อเนื่องทางธุรกิจ

แผนบริหารความเสี่ยง

วันที่มีผลบังคับใช้

ฉบับที่ 1, แก้ไขครั้งที่ 00

11 สิงหาคม 2569

อำนวยการบริหารความต่อเนื่องทางธุรกิจ (Business Continuity Management Steering Committee: BCMSC)

- ติดตามและดำเนินการแก้ไขข้อบกพร่องที่ตรวจพบจากเหตุการณ์และการกู้คืนระบบ รวมถึงปรับปรุงแผนกู้คืนระบบจากภัยพิบัติ (Disaster Recovery Plan: DRP) ขั้นตอนปฏิบัติ การตั้งค่าระบบ มาตรการควบคุม และข้อมูลการติดต่อที่เกี่ยวข้องให้เป็นปัจจุบัน

7. การจำแนกระดับความรุนแรงของเหตุการณ์ (Incident Severity Levels)

ระดับ	คำอธิบาย	ตัวอย่าง	การตอบสนอง
P1 - วิกฤต (Critical)	เหตุการณ์หรืออุบัติการณ์ที่ทำให้กระบวนการทางธุรกิจหรือระบบงานที่สำคัญหยุดชะงักทั้งหมดหรือในวงกว้าง และไม่สามารถดำเนินงานต่อไปได้ในระดับขั้นต่ำที่บริษัทฯ ยอมรับ หรือก่อให้เกิดหรือมีแนวโน้มก่อให้เกิดผลกระทบร้ายแรงต่อบุคลากร ทรัพย์สิน ข้อมูล ชื่อเสียง การปฏิบัติตามกฎหมาย หรือผู้มีส่วนได้เสียของบริษัทฯ	แผ่นดินไหว ไฟไหม้ น้ำท่วม โรคระบาด การก่อกวน หรือเหตุการณ์อื่นที่ส่งผลกระทบร้ายแรงต่อการดำเนินงาน รวมถึง Ransomware / Cyberattack ที่ทำให้ระบบหลัก เช่น SAP Production หรือ File Servers ถูกเข้ารหัสหรือไม่สามารถใช้งานได้ ในวงกว้าง หรือเกิดเหตุละเมิดข้อมูลที่มีความเสี่ยงสูง	ตอบสนองและรายงานโดยทันที พร้อมประเมินความจำเป็นในการประกาศใช้แผนกู้คืนระบบจากภัยพิบัติ (Disaster Recovery Plan: DRP) และ/หรือแผนความต่อเนื่องทางธุรกิจ (Business Continuity Plan: BCP) ตามลักษณะและผลกระทบของเหตุการณ์
P2 - สูง (High)	กระบวนการสำคัญหยุดชะงัก แต่ธุรกิจหลักยังสามารถดำเนินงานต่อไปในระดับจำกัด หรือเป็นการชั่วคราว โดยมีความเสี่ยงที่ผลกระทบจะขยายตัวหรือเกินระยะเวลาที่บริษัทฯ ยอมรับได้	ชุมชนประท้วงที่กระทบการเข้าถึงสถานที่ปฏิบัติงาน ระบบ M365 / Email หรือ File Server ล่ม ในวงกว้าง แต่ยังมีช่องทางหรือวิธีปฏิบัติงานทดแทนชั่วคราว	รับทราบ ประเมิน และเริ่มดำเนินการภายในสอง (2) ชั่วโมง นับแต่ทราบเหตุ และยกระดับเป็น P1 หากผลกระทบขยายตัว ไม่สามารถควบคุมได้ หรือมีแนวโน้มเกินเกณฑ์ที่กำหนดสำหรับ P1
P3 - ปานกลาง (Medium)	กระทบผู้ใช้ในวงจำกัด หรือระบบสนับสนุนที่ไม่วิกฤต โดยไม่กระทบต่อกระบวนการทางธุรกิจที่สำคัญอย่างมีนัยสำคัญ และมีวิธีปฏิบัติงานทดแทนที่เหมาะสม	ระบบ SAP สำหรับการพัฒนาและทดสอบ (SAP QAS / SAP DEV), ระบบเข้าแต่ยังทำงานได้	รับทราบ ประเมิน และเริ่มดำเนินการภายในสี่ (4) ชั่วโมงทำการ นับแต่ทราบเหตุ
P4 - ต่ำ (Low)	กระทบผู้ใช้หนึ่งถึงสอง (1-2) คน หรือปัญหาเล็กน้อยที่มีทางแก้ไขเฉพาะหน้า และไม่กระทบต่อความต่อเนื่องของกระบวนการทางธุรกิจที่สำคัญ	เครื่องพิมพ์เสีย ขอติดตั้งโปรแกรม ผู้ใช้ขอกำหนดรหัสผ่านใหม่	รับทราบและเริ่มดำเนินการภายในแปด (8) ชั่วโมงทำการ นับแต่ทราบเหตุ

การจัดระดับความรุนแรงของเหตุการณ์ให้พิจารณาจากลักษณะ ขอบเขต ระยะเวลา และผลกระทบที่เกิดขึ้นหรือคาดว่าจะเกิดขึ้นต่อบุคลากร กระบวนการทางธุรกิจ ระบบเทคโนโลยีสารสนเทศ ข้อมูล ทรัพย์สิน ชื่อเสียง การปฏิบัติตามกฎหมาย และผู้มีส่วนได้เสียของบริษัทฯ โดยประเภทของเหตุการณ์หรือตัวอย่างที่ระบุไว้ในตารางเป็นเพียงแนวทางประกอบการพิจารณาเท่านั้น

บริษัทฯ อาจปรับเปลี่ยนหรือลดระดับความรุนแรงของเหตุการณ์ได้ตามข้อมูลและสถานการณ์ที่เปลี่ยนแปลงไป และต้องรายงานการปรับระดับดังกล่าวต่อผู้มีอำนาจและคณะกรรมการที่เกี่ยวข้องโดยทันที

8. การทบทวนนโยบาย บทบาท หน้าที่ และความรับผิดชอบ และกรอบการบริหารความต่อเนื่องทางธุรกิจ (Continual Improvement of Business Continuity Management)

คณะกรรมการอำนวยการบริหารความต่อเนื่องทางธุรกิจ (Business Continuity Management Steering Committee: BCMSC) จะต้องดำเนินการทบทวนนโยบาย บทบาท หน้าที่ และความรับผิดชอบ และกรอบการบริหารความต่อเนื่องทางธุรกิจ รวมถึงแผนความต่อเนื่องทางธุรกิจ (Business Continuity Plan: BCP) และแผนที่เกี่ยวข้อง ปีละหนึ่ง (1) ครั้ง และเมื่อมีการเปลี่ยนแปลงหรือเหตุการณ์ที่มีนัยสำคัญ โดยพิจารณาจากข้อมูลนำเข้า เช่น ผลการทดสอบแผน เหตุการณ์หยุดชะงักที่ผ่านมา การประเมินความเสี่ยง (Risk Assessment: RA) และการวิเคราะห์ผลกระทบทางธุรกิจ (Business Impact Analysis: BIA) รวมถึงการเปลี่ยนแปลงด้านธุรกิจ ด้านเทคโนโลยี และข้อกำหนดทางกฎหมาย หรือข้อกำหนดอื่นที่เกี่ยวข้อง

ผลการทบทวนดังกล่าวต้องนำมาใช้ในการปรับปรุงนโยบาย แผนงาน และกระบวนการที่เกี่ยวข้อง พร้อมกำหนดแผนการดำเนินงาน ผู้รับผิดชอบ และระยะเวลาการดำเนินการอย่างชัดเจน รวมทั้งมีการติดตามผลและรายงานต่อผู้บริหารระดับสูงตามระยะเวลาที่เหมาะสม รวมถึงจัดให้มีการบันทึกและจัดเก็บหลักฐานที่เกี่ยวข้องเพื่อเป็นข้อมูลในการทบทวน และปรับปรุงในรอบถัดไปได้อย่างต่อเนื่องและมีประสิทธิภาพ

หมายเหตุ :

- ผู้บริหาร และพนักงานทุกระดับมีส่วนร่วมในการสนับสนุน และผลักดันให้บริษัทฯ ตระหนัก และให้ความสำคัญต่อการดำเนินงานตามระบบการบริหารความต่อเนื่องทางธุรกิจ (Business Continuity Management System: BCMS)
- พนักงานและบุคลากรทุกคนมีหน้าที่ศึกษา ทำความเข้าใจ และปฏิบัติตามนโยบายการบริหารความต่อเนื่องทางธุรกิจ (Business Continuity Management Policy: BCMP) ฉบับนี้ รวมถึงบทบาท หน้าที่ และความรับผิดชอบที่เกี่ยวข้องกับตน

9. เอกสารอ้างอิง (Reference)

ลำดับ	รหัสเอกสาร	รายการอ้างอิง
1.		แผนผังข้อมูลโครงสร้างบริษัทฯ วันที่ 1 ตุลาคม พ.ศ.2568
2.	RM003	แผนความต่อเนื่องทางธุรกิจ (Business Continuity Plan)
3.	BCP-ITS-001	แผนการบริหารจัดการความต่อเนื่องทางธุรกิจและการกู้คืนระบบสารสนเทศ (Business Continuity Management and IT Disaster Recovery Plan)
4.	SOP-ITS-001	ขั้นตอนปฏิบัติและการบริหารจัดการความต่อเนื่องทางธุรกิจและการกู้คืนระบบสารสนเทศ (Business Continuity Management and IT Disaster Recovery Procedure)
5.		แผนตอบสนองอุบัติการณ์ (Incident Response Plan)
6.		รายงานการวิเคราะห์ผลกระทบทางธุรกิจ (Business Impact Analysis Report)
7.		รายงานผลการประเมินความเสี่ยง (Risk Assessment Report)

10. บันทึกการแก้ไข (Revision History)

บันทึกการแก้ไข			
ฉบับที่	วันที่	จัดทำ/แก้ไขปรับปรุง	เนื้อหา/เหตุผลที่แก้ไข
1	11 สิงหาคม 2569	แผนกบริหารความเสี่ยง	จัดทำครั้งแรก