ประมวลแนวทางปฏิบัติและกรอบมาตรฐาน ด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ ของสถาบันระหว่างประเทศเพื่อการค้าและการพัฒนา (องค์การมหาชน)

พ.ศ. 2569

ฉบับทบทวน



กลุ่มงานสารสนเทศ สำนักยุทธศาสตร์และสารสนเทศ
สถาบันระหว่างประเทศเพื่อการค้าและการพัฒนา (องค์การมหาชน)

สารบัญ

๑. บทนำ ๖

๒. วัตถุประสงค์ ๗

๓. ขอบเขตการใช้งาน ๗

๔. คำนิยาม ๗

๕. การจัดทำมาตรฐานและแนวปฏิบัติด้านความมั่นคงปลอดภัยทางไซเบอร์ของสถาบันระหว่างประเทศเพื่อการค้าและการพัฒนา (องค์การมหาชน) มี ๓ ส่วน ดังนี้ ๙

ส่วนที่ ๑ มาตรฐานการกำหนดคุณลักษณะความมั่นคงปลอดภัยไซเบอร์ให้แก่ข้อมูลหรือระบบสารสนเทศ พ.ศ. ๒๕๖๘ ๙

ส่วนที่ ๒ ประมวลแนวทางปฏิบัติการรักษาความมั่นคงปลอดภัยไซเบอร์ ๑๔

๑. แผนการตรวจสอบด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ ๑๔

๒. การประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ ๑๔

๓. แผนการรับมือภัยคุกคามทางไซเบอร์ ๑๕

๔. การรายงานสถานการณ์เกี่ยวกับด้านความมั่นคงปลอดภัยไซเบอร์ ๑๖

ส่วนที่ ๓ กรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ ๑๖

หัวข้อที่ ๑ การระบุความเสี่ยงที่อาจจะเกิดขึ้นแก่คอมพิวเตอร์ ข้อมูลคอมพิวเตอร์ ระบบคอมพิวเตอร์ ข้อมูลอื่นที่เกี่ยวข้องกับระบบคอมพิวเตอร์ ทรัพย์สินและชีวิตร่างกายของบุคคล (Identify) ๑๖

๑.๑ การจัดการทรัพย์สิน (Asset Management) ๑๖

๑.๒ การประเมินความเสี่ยงและกลยุทธ์ในการจัดการความเสี่ยง (Risk Assessment and Risk Management Strategy) ๑๗

หัวข้อที่ ๒ มาตรการป้องกันความเสี่ยงที่อาจจะเกิดขึ้น (Protect) ๑๗

๒.๑ การควบคุมการเข้าถึง (Access Control) ๑๗

๒.๒ การทำให้ระบบมีความแข็งแกร่ง (System Hardening) ๑๘

๒.๓ การสร้างความตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Awareness) ๑๙

หัวข้อที่ ๓ มาตรการตรวจสอบและเฝ้าระวังภัยคุกคามทางไซเบอร์ (Detect) ๑๙

หัวข้อที่ ๔ มาตรการเผชิญเหตุเมื่อมีการตรวจพบภัยคุกคามทางไซเบอร์ (Respond) ๒๐

๔.๑ แผนการรับมือภัยคุกคามทางไซเบอร์ (Cybersecurity Incident Response Plan) ๒๐

๔.๒ แผนการสื่อสารในภาวะวิกฤต (Crisis Communication Plan) ๒๐

หัวข้อที่ ๕ มาตรการรักษาและฟื้นฟูความเสียหายที่เกิดจากภัยคุกคามทางไซเบอร์ (Cybersecurity Resilience and Recovery) ๒๐

๕.๑ สถาบันต้องจัดทำแผนความต่อเนื่องทางธุรกิจ (Business Continuity Plan : BCP) ๒๑

๕.๒ สถาบันต้องตรวจสอบให้แน่ใจว่ามีการฝึกซ้อมแผนความต่อเนื่องธุรกิจ ๒๑

๕.๓ ในกรณีตรวจพบภัยคุกคามทางไซเบอร์ (Cyber Security Incident) ๒๑

ภาคผนวก ๒๓

แผนความต่อเนื่องทางธุรกิจ (Business Continuity Plan) ด้านเทคโนโลยีสารสนเทศ ๒๔

๑. บทนำ ๒๖

๒. ภูมิหลังของสถาบัน ๒๘

๓. การกำกับดูแลและนโยบายการบริหารความต่อเนื่องทางธุรกิจ (Business Continuity Management: BCM) ๓๐

๔. ทบทวนแผนและบำรุงรักษา ๓๒

๕. การฝึกอบรมและการฝึกซ้อมแผน ๓๒

๖. ลำดับความสำคัญและกลยุทธ์ความต่อเนื่องทางธุรกิจ ๓๒

๗. การเปิดใช้งานแผน ๓๙

๘. การตอบสนองของสถาบัน ๔๐

๙. กลยุทธ์การสื่อสาร ๔๑

๑๐. ภาคผนวกที่เกี่ยวกับการทำงาน ๔๒

สารบัญตาราง

ประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

ตารางที่ ๑ ระดับผลกระทบที่อาจเกิดขึ้นในแต่ละระดับตามวัตถุประสงค์ด้านความมั่นคงปลอดภัยไซเบอร์ (Security Objectives) ๑๐

ตารางที่ ๒ สรุประดับคุณลักษณะความมั่นคงปลอดภัยไซเบอร์และหัวข้อมาตรการควบคุมความมั่นคงปลอดภัยไซเบอร์ขั้นต่ำสำหรับข้อมูลหรือระบบสารสนเทศ ๑๒

แผนความต่อเนื่องทางธุรกิจ

ตารางที่ ๑ ตารางหน้าที่ทางธุรกิจที่สำคัญ (Critical Business Functions) ๓๔

ตารางที่ ๒ ตารางบริการสำคัญและประเภทของการพึ่งพา (Type of Dependency) ๓๘

ตารางที่ ๓ ตารางการกำหนดหน้าที่รับผิดชอบการประสานงาน ๔๑

ตารางที่ ๔ การสื่อสารกับผู้มีส่วนได้ส่วนเสียที่เกี่ยวข้อง ๔๒

ตารางที่ ๕ รายชื่อสมาชิกในทีม (Business Continuity Team Members) ๔๕

ตารางที่ ๖ จุดควบคุมเหตุภัยคุกคามทางไซเบอร์ (Incident Control Point) ๔๕

ตารางที่ ๗ การดำเนินการทันที (Immediate) ๔๖

ตารางที่ ๘ แบบตารางการดำเนินการต่อเนื่องของสถาบัน ๔๖

ตารางที่ ๙ การดำเนินการหลังเหตุภัยคุกคามทางไซเบอร์ของสถาบัน ๔๗

ตารางที่ ๑๐ การติดต่อภายใน ๔๘

ตารางที่ ๑๑ การติดต่อภายนอก ๔๙

ตารางที่ ๑๒ ฟังก์ชันที่สำคัญ (Critical Functions) ของสถาบัน ๕๒

ตารางที่ ๑๔ กลยุทธ์ความต่อเนื่องทางธุรกิจ (Business Continuity Strategies) ต่อระบบของสถาบัน ๕๓

ตารางที่ ๑๕ การดำเนินการทันที (Immediate) ๕๔

ตารางที่ ๑๖ การดำเนินการต่อเนื่อง (On-going) ๕๕

ตารางที่ ๑๗ การดำเนินการหลังเหตุภัยคุกคามทางไซเบอร์ (Post-Incident) ๕๖

ตารางที่ ๑๘ ตารางความต้องการทรัพยากรบุคลากร (People) ๕๖

ตารางที่ ๑๙ ตารางความต้องการทรัพยากร (Resource Requirements) ๕๗

ตารางที่ ๒๐ ตารางระบบ/แอปพลิเคชัน (Systems/ Applications) ๕๘

ตารางที่ ๒๑ ให้บริการกับฟังก์ชันการทำงานที่สำคัญ (Upstream Interdependencies) ๕๘

ตารางที่ ๒๒ ใช้บริการจากฟังก์ชันการทำงานทางธุรกิจ (Downstream Interdependencies) ๖๐

ตารางที่ ๒๓ ภัยคุกคามและอันตรายที่อาจเกิดขึ้นต่อระบบสารสนเทศ ๖๑

ตารางที่ ๒๔ การกำหนดกระบวนการทางธุรกิจ ๖๒

ตารางที่ ๒๕ ระดับการพิจารณาผลกระทบ ๖๓
ตารางที่ ๒๖ การประเมินผลกระทบด้านต่าง ๆ และระดับผลกระทบต่อบริการที่สำคัญ ๖๔
ตารางที่ ๒๗ คุณลักษณะความมั่นคงปลอดภัยไซเบอร์ของระบบสารสนเทศที่ใช้สนับสนุนกระบวนการชำระหนี้ ๖๖
ตารางที่ ๒๘ สถาบันระบุระยะเวลา MTD RTO และ RPO ดังตารางต่อไปนี้ ๖๖
ตารางที่ ๒๙ ระบุทรัพยากรที่เกี่ยวข้องกับกระบวนการทางธุรกิจที่ต้องใช้ในการดำเนินการ ๖๗

สารบัญรูปภาพ

รูปที่ ๑ ประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ ๑๕
รูปที่ ๒ ความสัมพันธ์ระหว่างเหตุ (Incident) และระยะเวลาเป้าหมายในการกู้คืนบริการที่สำคัญ ๓๓
รูปที่ ๓ ภาพแสดงขั้นตอนความต่อเนื่องของการตอบสนองตั้งแต่เกิดการหยุดชะงัก ไปจนถึงหยุดทำงาน ๔๐
รูปที่ ๔ ภาพโครงสร้างของทีมความต่อเนื่องทางธุรกิจ (Business Continuity Team: BCT) ๔๓
รูปที่ ๕ ภาพแสดงกระบวนการวิเคราะห์ผลกระทบทางธุรกิจ ๕๙

ประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์
ของสถาบันระหว่างประเทศเพื่อการค้าและการพัฒนา (องค์การมหาชน)
ฉบับทบทวน พ.ศ. ๒๕๖๙

๑. บทนำ

พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ ได้บัญญัติให้มีโครงสร้างการกำกับดูแลและมาตรการรักษาความมั่นคงปลอดภัยไซเบอร์ระดับชาติ โดยกำหนดให้หน่วยงานของรัฐ สถาบันควบคุมหรือกำกับดูแล และสถาบันโครงสร้างพื้นฐานสำคัญทางสารสนเทศ ดำเนินการจัดทำประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ เพื่อใช้เป็นข้อกำหนดขั้นต่ำ (Security Control Baseline) ในการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศและเครือข่ายคอมพิวเตอร์ ทั้งนี้ เพื่อให้การบริหารจัดการความเสี่ยง การเฝ้าระวัง ตรวจสอบ การตอบสนอง และการรับมือกับภัยคุกคามทางไซเบอร์เป็นไปด้วยความรวดเร็ว มีประสิทธิภาพ สอดคล้องกับมาตรฐานสากล และเป็นไปในทิศทางเดียวกันทั่วประเทศ ซึ่งสอดรับกับนโยบายและแผนปฏิบัติการว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ (พ.ศ. ๒๕๖๕ - ๒๕๗๐) ที่คณะรัฐมนตรีให้ความเห็นชอบให้เป็นแผนแม่บทระดับชาติ เพื่อสร้างความยืดหยุ่นและการฟื้นตัวอย่างรวดเร็ว ให้แก่บริการที่สำคัญของประเทศ

สถาบันระหว่างประเทศเพื่อการค้าและการพัฒนา (องค์การมหาชน) ในฐานะหน่วยงานของรัฐที่มีภารกิจสำคัญในการส่งเสริมการค้า การพัฒนา และการให้บริการทางอิเล็กทรอนิกส์แก่ภาคธุรกิจ บุคลากรภาครัฐ และสาธารณชน ได้เล็งเห็นถึงความสำคัญของการสร้างระบบนิเวศดิจิทัลที่มีความมั่นคงปลอดภัย น่าเชื่อถือ และพร้อมใช้งานได้อย่างต่อเนื่อง จึงได้ดำเนินการจัดทำและปรับปรุงประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ สถาบันระหว่างประเทศเพื่อการค้าและการพัฒนา (องค์การมหาชน) ฉบับทบทวน พ.ศ. ๒๕๖๙ ขึ้น เพื่อเป็นกรอบการดำเนินงานหลักสำหรับผู้บริหาร เจ้าหน้าที่สารสนเทศ ผู้ดูแลระบบ บุคลากรภายในองค์กร ตลอดจนผู้ให้บริการภายนอกให้สามารถปฏิบัติงานได้อย่างถูกต้อง ปลอดภัย และสอดคล้องกับเงื่อนไขทางกฎหมายอย่างเคร่งครัด

การจัดทำเอกสารฉบับทบทวน พ.ศ. ๒๕๖๙ นี้ ถือเป็นกลไกสำคัญในการยกระดับมาตรฐานด้านความมั่นคงปลอดภัยสารสนเทศของสถาบันให้เท่าทันต่อการเปลี่ยนแปลงเชิงสถาปัตยกรรมเทคโนโลยี และการย้ายระบบงานหลักไปสู่ระบบคลาวด์ภาครัฐ (GDCC) และระบบคลาวด์ภายนอก ได้แก่ ระบบบริหารจัดการสำนักงาน ระบบบริหารจัดการงบประมาณและบัญชี ระบบ Prompt Pass ระบบจัดการบุคลากร และระบบเว็บไซต์สถาบัน ซึ่งส่งผลให้รูปแบบความเสี่ยงทางไซเบอร์มีความซับซ้อนมากยิ่งขึ้น สถาบันจึงจำเป็นต้องปรับปรุงมาตรการควบคุมความมั่นคงปลอดภัยให้ครอบคลุมตาม ประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง มาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ระบบคลาวด์ พ.ศ. ๒๕๖๗

นอกจากนี้ การปรับปรุงนโยบายเป็นฉบับ พ.ศ. ๒๕๖๙ ยังตอบสนองต่อการเปลี่ยนแปลงของภัยคุกคามทางไซเบอร์อุบัติใหม่ ที่มีความรุนแรงและแยบยลยิ่งขึ้น เช่น มัลแวร์เรียกไถ่เชิงลึก การโจมตีห่วงโซ่อุปทานเทคโนโลยี ควบคู่ไปกับการปรับปรุงข้อบังคับภายในให้สอดคล้องกับกฎหมายลำดับรองและประกาศฉบับใหม่ของสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.) เพื่อให้สถาบันมีความพร้อมสมบูรณ์ในการรองรับการติดตามประเมินผลสัมฤทธิ์ตามแผนปฏิบัติการระดับชาติต่อไป

๒. วัตถุประสงค์

ประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ฉบับนี้ จัดทำขึ้นโดยมีวัตถุประสงค์สำคัญ ดังนี้

๒.๑ เพื่อกำหนดกรอบแนวทางและมาตรการในการรักษาความมั่นคงปลอดภัยไซเบอร์ ให้สามารถตอบสนองและรับมือกับภัยคุกคามทางไซเบอร์ได้อย่างรวดเร็วทันท่วงที และพร้อมใช้งานได้อย่างต่อเนื่อง

๒.๒ เพื่อยกระดับการบริหารจัดการระบบสารสนเทศและเทคโนโลยีดิจิทัลของสถาบัน ให้มีประสิทธิภาพ มีความมั่นคงปลอดภัย และสอดคล้องตามเกณฑ์มาตรฐานภาครัฐ

๒.๓ เพื่อให้การปฏิบัติงานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของบุคลากรและเจ้าหน้าที่ภายในสถาบันเป็นไปในทิศทางเดียวกันอย่างมีเอกภาพ และถูกต้องตามข้อกำหนดของพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ และระเบียบที่เกี่ยวข้อง

๓. ขอบเขตการใช้

ประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ฉบับนี้ มีผลบังคับใช้ครอบคลุมข้อมูล และระบบสารสนเทศของสถาบันระหว่างประเทศเพื่อการค้าและการพัฒนา (องค์การมหาชน)

๔. คำนิยาม

๑. สถาบัน	หมายถึง	สถาบันระหว่างประเทศเพื่อการค้าและการพัฒนา (องค์การมหาชน)
๒. ผู้บังคับบัญชา	หมายถึง	ผู้อำนวยการ สถาบันระหว่างประเทศเพื่อการค้าและการพัฒนา
๓. ผู้บริหารเทคโนโลยีสารสนเทศระดับสูง ระดับกรม (Department Chief Information Officer: DCIO)	หมายถึง	รองผู้อำนวยการ (วิชาการ) ที่ได้รับมอบหมายซึ่งมีหน้าที่รับผิดชอบการกำหนดนโยบายและมาตรฐานการควบคุมดูแลการใช้งานและพัฒนาระบบเทคโนโลยีสารสนเทศของสถาบันระหว่างประเทศเพื่อการค้าและการพัฒนา (องค์การมหาชน)
๔. กลุ่มงานสารสนเทศ	หมายถึง	กลุ่มงานสารสนเทศ สำนักยุทธศาสตร์และสารสนเทศ ซึ่งเป็นสถาบันให้บริการเทคโนโลยีสารสนเทศ ให้คำปรึกษา พัฒนา ปรับปรุง และบำรุงรักษาระบบคอมพิวเตอร์ และเครือข่ายภายในสถาบันระหว่างประเทศเพื่อการค้าและการพัฒนา (องค์การมหาชน)
๕. หัวหน้ากลุ่มงานสารสนเทศ	หมายถึง	ผู้อำนวยการ สำนักยุทธศาสตร์และสารสนเทศ รับผิดชอบกำกับดูแลการปฏิบัติงานของบุคลากร ตลอดจนทบทวน วางแผนบริหารจัดการความเสี่ยงระบบเทคโนโลยีสารสนเทศ
๖. ผู้ใช้งาน	หมายถึง	บุคลากรของสถาบันระหว่างประเทศเพื่อการค้าและการพัฒนา (องค์การมหาชน) ที่ได้รับอนุญาต (Authorized user) ให้สามารถใช้งานระบบเทคโนโลยีสารสนเทศโดยมีสิทธิ

		และหน้าที่ขึ้นอยู่กับบทบาทความรับผิดชอบ (Role)
๗. ผู้ให้บริการภายนอก	หมายถึง	องค์กร สถาบัน บริษัทหรือบุคคล ซึ่งเป็นผู้ให้บริการหรือผู้มาติดต่อจากภายนอกที่สถาบันอนุญาตให้มีสิทธิในการเข้าถึง และใช้งานระบบหรือทรัพย์สินต่าง ๆ ของสถาบันระหว่างประเทศเพื่อการค้าและการพัฒนา (องค์การมหาชน) โดยจะได้รับสิทธิในการใช้ เข้าถึงข้อมูล บริการ และการใช้งานระบบสารสนเทศตามอำนาจหน้าที่ และต้องรับผิดชอบในการรักษาความมั่นคงปลอดภัยของสารสนเทศและความลับของข้อมูล
๘. คอมไพเลอร์	หมายถึง	โปรแกรมแปลโปรแกรม ตัวแปลงโปรแกรม เป็นโปรแกรมคอมพิวเตอร์ที่ทำหน้าที่แปลงชุดคำสั่งภาษาคอมพิวเตอร์หนึ่งไปเป็นชุดคำสั่งที่มีความหมายเดียวกันในภาษาคอมพิวเตอร์อื่น
๙. แพตช์	หมายถึง	โปรแกรมที่ใช้ในการปรับปรุงแก้ไขซอฟต์แวร์ โดยส่วนใหญ่อยู่ในลักษณะของไฟล์ และใช้เพื่อแก้ไขช่องโหว่เรื่องความมั่นคงปลอดภัย หรือเพื่อเพิ่มความสามารถของซอฟต์แวร์ ผู้พัฒนาซอฟต์แวร์หลายรายได้เผยแพร่แพตช์ออกมาเป็นระยะ เช่น บริษัท Microsoft จะเผยแพร่แพตช์ที่แก้ไขช่องโหว่ของซอฟต์แวร์ผ่านระบบ Windows Update
๑๐. Recovery Time Objective (RTO)	หมายถึง	ระยะเวลาในการกู้คืนระบบ
๑๑. Recovery Point Objective (RPO)	หมายถึง	ระยะเวลาสูงสุดที่ยอมให้ข้อมูลเสียหาย
๑๒. Maximum Tolerance Period of Disruption (MTPD)	หมายถึง	ระยะเวลาสูงสุดที่ยอมให้ธุรกิจหยุดชะงักเพื่อรองรับการดำเนินธุรกิจอย่างต่อเนื่องของสถาบัน และรองรับการเกิดเหตุการณ์ผิดปกติต่าง ๆ ที่อาจส่งผลให้เกิดการหยุดชะงัก หรือเกิดความเสียหายต่อระบบ เช่น ภัยคุกคามการทำงานได้ตามปกติให้เร็วที่สุด
๑๓. Business Continuity Plan (BCP)	หมายถึง	แผนบริหารความต่อเนื่องทางธุรกิจ

๕. การจัดทำมาตรฐานและแนวทางปฏิบัติด้านความมั่นคงปลอดภัยไซเบอร์ของสถาบันระหว่างประเทศเพื่อการค้าและการพัฒนา (องค์การมหาชน) มี ๓ ส่วน ดังนี้

ส่วนที่ ๑
มาตรฐานการกำหนดคุณลักษณะความมั่นคงปลอดภัยไซเบอร์ ให้แก่ข้อมูลหรือระบบสารสนเทศ พ.ศ. ๒๕๖๘

๑. การประเมินระดับผลกระทบของข้อมูลหรือระบบสารสนเทศ

๑.๑ กฎหมายที่เกี่ยวข้อง

๑.๑.๑ ตามประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (กมช.) เรื่อง มาตรฐานการกำหนดคุณลักษณะความมั่นคงปลอดภัยไซเบอร์ให้แก่ข้อมูลหรือระบบสารสนเทศ พ.ศ. ๒๕๖๖

ข้อ ๔ กำหนดให้สถาบันกำหนดคุณลักษณะความมั่นคงปลอดภัยไซเบอร์ให้แก่ข้อมูลหรือระบบสารสนเทศ โดยพิจารณาวัตถุประสงค์ด้านความมั่นคงปลอดภัยไซเบอร์ (Security Objectives) ในเรื่อง

๑) การรักษาความลับ (Confidentiality) หมายถึง การรักษาหรือสงวนไว้ซึ่งการจำกัดการเข้าถึงหรือการเปิดเผยข้อมูลให้แก่บุคคล สถาบันอื่น หรือชุดคำสั่งที่ไม่ได้รับอนุญาต

๒) การรักษาความถูกต้องครบถ้วน (Integrity) หมายถึง การรักษาหรือสงวนไว้ซึ่งความถูกต้องและความครบถ้วนของข้อมูล

๓) การรักษาสภาพพร้อมใช้งาน (Availability) หมายถึง การดำเนินการ เพื่อให้บุคคล สถาบัน หรือชุดคำสั่งที่ได้รับอนุญาตสามารถเข้าถึงและใช้งานข้อมูลหรือระบบสารสนเทศได้ตามต้องการและได้อย่างมีประสิทธิภาพ

ข้อ ๕ การพิจารณาวัตถุประสงค์ตามข้อ ๔ วรรคหนึ่ง (๑) (๒) และ (๓) ให้ประเมินและจัดระดับผลกระทบที่อาจเกิดขึ้นเป็นสามระดับ ได้แก่ ระดับต่ำ ระดับกลาง และระดับสูง

ข้อ ๖ การจัดระดับผลกระทบที่อาจเกิดขึ้นในแต่ละระดับตามข้อ ๕ ให้พิจารณาการประเมินผลกระทบในแต่ละด้าน

๑.๑.๒ ตามประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง มาตรฐานขั้นต่ำของข้อมูลหรือระบบสารสนเทศ พ.ศ. ๒๕๖๖

ข้อ ๔ กำหนดให้ภายหลังจากสถาบันได้กำหนดคุณลักษณะความมั่นคงปลอดภัยไซเบอร์ให้แก่ข้อมูลหรือระบบสารสนเทศ ซึ่งพิจารณาจากวัตถุประสงค์ด้านความมั่นคงปลอดภัยไซเบอร์ในเรื่องการรักษาความลับ การรักษาความถูกต้องครบถ้วน และการรักษาสภาพพร้อมใช้งาน และได้ระดับผลกระทบที่อาจเกิดขึ้นตามวัตถุประสงค์แต่ละเรื่องเป็นระดับต่ำ ระดับกลาง หรือระดับสูง ตามประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง มาตรฐานการกำหนดคุณลักษณะความมั่นคงปลอดภัยไซเบอร์ให้แก่ข้อมูลหรือระบบสารสนเทศแล้ว ให้สถาบันกำหนดมาตรการควบคุมความมั่นคงปลอดภัยไซเบอร์ขั้นต่ำ สำหรับข้อมูลหรือระบบสารสนเทศนั้นในแต่ละระดับตามหัวข้อประกาศคณะกรรมการกำกับดูแลด้านความ

มั่นคงปลอดภัยไซเบอร์ เรื่อง ประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์สำหรับหน่วยงานของรัฐและสถาบันโครงสร้างพื้นฐานสำคัญทางสารสนเทศ

๑.๒ เกณฑ์การประเมินระดับผลกระทบที่อาจเกิดขึ้นตามวัตถุประสงค์ด้านความมั่นคงปลอดภัยไซเบอร์ (Security Objectives)

สถาบันได้กำหนดเกณฑ์การประเมินระดับผลกระทบที่อาจเกิดขึ้นในแต่ละระดับ โดยพิจารณาจากวัตถุประสงค์ด้านความมั่นคงปลอดภัยไซเบอร์ (Security Objectives) ในแต่ละเรื่องตามประกาศ กมช. เรื่อง มาตรฐานการกำหนดคุณลักษณะความมั่นคงปลอดภัยไซเบอร์ให้แก่ข้อมูลหรือระบบสารสนเทศ พ.ศ. ๒๕๖๖ ซึ่งสามารถสรุปได้ดังนี้

ตารางที่ ๑ ระดับผลกระทบที่อาจเกิดขึ้นในแต่ละระดับตามวัตถุประสงค์ด้านความมั่นคงปลอดภัยไซเบอร์ (Security Objectives)[๑]

วัตถุประสงค์ด้านความมั่นคงปลอดภัยไซเบอร์ (Security Objectives)	**ผลกระทบ (Impact)* และ ผลประโยชน์แห่งชาติ (National Interests)**		
	ระดับต่ำ	**ระดับกลาง**	**ระดับสูง**
ด้านความลับ (Confidentiality) การรักษาข้อจำกัดในการได้รับอนุญาตให้เข้าถึงได้และเปิดเผยเฉพาะผู้มีสิทธิ์ รวมทั้งวิธีการคุ้มครองความเป็นส่วนตัว (Privacy) และกรรมสิทธิ์ (Proprietary) ของข้อมูลข่าวสาร	การเปิดเผยข้อมูลโดยไม่ได้รับอนุญาตอาจส่งผลกระทบน้อย/อย่างจำกัด (Limited) และเกิดผลประโยชน์แห่งชาติสำคัญน้อย (Less Important or Secondary National Interests)	การเปิดเผยข้อมูลโดยไม่ได้รับอนุญาตอาจส่งผลกระทบอย่างร้ายแรง (Serious) และเกิดผลประโยชน์แห่งชาติที่สำคัญ (Important National Interests)	การเปิดเผยข้อมูลโดยไม่ได้รับอนุญาตอาจส่งผลกระทบอย่างร้ายแรงมาก (Severe or Catastrophic) และเกิดผลประโยชน์แห่งชาติสำคัญยิ่ง (Extremely Important National Interests)
ด้านความถูกต้องครบถ้วน (Integrity) การปกป้องจากการดัดแปลงหรือทำลายข้อมูลที่ไม่เหมาะสม และรวมถึงการรับรองว่าข้อมูลจะไม่ถูกปฏิเสธ (Non-Repudiation) และเป็นข้อมูลที่ถูกต้องเป็นความจริง (Authenticity)	การแก้ไขหรือทำลายข้อมูลโดยไม่ได้รับอนุญาตอาจส่งผล กระทบน้อย/อย่างจำกัด (Limited) และเกิดผลประโยชน์แห่งชาติสำคัญน้อย (Less Important or Secondary National Interests)	การแก้ไขหรือทำลายข้อมูลโดยไม่ได้รับอนุญาตอาจส่งผลกระทบอย่างร้ายแรง (Serious) และเกิดผลประโยชน์แห่งชาติที่สำคัญ (Important National Interests)	การแก้ไขหรือทำลายข้อมูลโดยไม่ได้รับอนุญาตอาจส่งผลกระทบอย่างร้ายแรงมาก (Severe or Catastrophic) และเกิดผลประโยชน์แห่งชาติสำคัญยิ่ง (Extremely Important National Interests)
ด้านความพร้อมใช้งาน (Availability) การสร้างความมั่นใจในการเข้าถึง และการใช้	การหยุดชะงักของการเข้าถึงหรือการใช้ข้อมูลข่าวสารหรือระบบสารสนเทศอาจส่งผลกระทบน้อย/อย่างจำกัด (Limited) และเกิด	การหยุดชะงักของการเข้าถึงหรือการใช้ข้อมูลข่าวสารหรือระบบสารสนเทศอาจส่งผลกระทบอย่างร้ายแรง (Serious) และเกิด	การหยุดชะงักของการเข้าถึงหรือการใช้ข้อมูลข่าวสารหรือระบบสารสนเทศอาจส่งผลกระทบอย่างร้ายแรงมาก (Severe or

[๑] อ้างอิงตามประกาศสำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน) ที่ ม 1/2565 เรื่อง มาตรฐานสำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน) ว่าด้วยหลักเกณฑ์การจัดระดับชั้นและแบ่งปันข้อมูลภาครัฐ

วัตถุประสงค์ด้านความมั่นคงปลอดภัยไซเบอร์ (Security Objectives)	ผลกระทบ (Impact)* และ ผลประโยชน์แห่งชาติ (National Interests)		
	ระดับต่ำ	ระดับกลาง	ระดับสูง
ข้อมูลอย่างทันท่วงที/เป็นปัจจุบันและเชื่อถือได้	ผลประโยชน์แห่งชาติสำคัญน้อย (Less Important or Secondary National Interests)	ผลประโยชน์แห่งชาติที่สำคัญ (Important National Interests)	Catastrophic) และเกิดผลประโยชน์แห่งชาติ สำคัญยิ่ง (Extremely Important National Interests)

๑.๓ สรุปผลการประเมินระดับผลกระทบที่อาจเกิดขึ้นตามวัตถุประสงค์ด้านความมั่นคงปลอดภัยไซเบอร์ (Security Objectives) และการรับรองมาตรฐานการรักษาความมั่นคงปลอดภัยไซเบอร์ระบบคลาวด์

๑.๓.๑ ผลการประเมินระดับผลกระทบที่อาจเกิดขึ้นของสถาบันตามวัตถุประสงค์ด้านความมั่นคงปลอดภัยไซเบอร์ (Security Objectives)

๑) ด้านการรักษาความลับ (Confidentiality) หมายถึง การทำให้แน่ใจว่าข้อมูลที่ละเอียดอ่อน ข้อมูลส่วนบุคคล หรือข้อมูลที่เป็นกรรมสิทธิ์ของสถาบันจะไม่ถูกเปิดเผยต่อบุคคลภายในและภายนอกที่ไม่ได้รับอนุญาต ซึ่งระดับผลกระทบของการละเมิดการรักษาความลับขึ้นอยู่กับความสำคัญของข้อมูลที่ถูกเปิดเผยและสถานการณ์ของการละเมิด ทั้งนี้ เมื่อพิจารณาข้อมูลหรือระบบสารสนเทศของสถาบัน พบว่า ข้อมูลที่สถาบันจัดเก็บไม่มีลักษณะเป็นความลับหรือข้อมูลที่มีความอ่อนไหวสูง ไม่ใช่ข้อมูลลับของทางราชการหรือเป็นภัยต่อความมั่นคงของรัฐ ทั้งนี้ ผลกระทบที่อาจเกิดขึ้นจึงอยู่ใน “ระดับต่ำ”

๒) การรักษาความถูกต้องครบถ้วน (Integrity) หมายถึง การรับประกันว่าข้อมูลและระบบมีความถูกต้อง สมบูรณ์ เชื่อถือได้ และได้รับการปกป้องจากการแก้ไขเปลี่ยนแปลงหรือการทำลายโดยไม่ได้รับอนุญาต ทั้งนี้ เมื่อพิจารณาข้อมูลหรือระบบสารสนเทศของสถาบัน พบว่า ข้อมูลที่สถาบันจัดเก็บส่วนใหญ่เกี่ยวข้องกับภารกิจด้านการฝึกอบรม ประชุม และสัมมนา ซึ่งไม่ส่งผลกระทบต่อการดำเนินงานหรือการตัดสินใจ ทั้งนี้ ผลกระทบที่อาจเกิดขึ้นจึงอยู่ใน “ระดับต่ำ”

๓) การรักษาสภาพพร้อมใช้งาน (Availability) หมายถึง การที่ผู้มีสิทธิ์ไม่สามารถเข้าถึงข้อมูลหรือระบบได้ตามต้องการ ซึ่งอาจนำไปสู่ผลกระทบที่สำคัญหลายประการ ทั้งนี้ เมื่อพิจารณาข้อมูลหรือระบบสารสนเทศของสถาบัน พบว่า ข้อมูลที่สถาบันมิใช่ข้อมูลที่มีความสำคัญสูงหรือเป็นข้อมูลที่หากสูญหายจะส่งให้ผลการดำเนินงานหยุดชะงัก ทั้งนี้ ผลกระทบที่อาจเกิดขึ้นจึงอยู่ใน “ระดับต่ำ”

๑.๓.๒ มาตรการควบคุมความมั่นคงปลอดภัยไซเบอร์

การตรวจรับรองมาตรฐานการรักษาความมั่นคงปลอดภัยไซเบอร์สำหรับระบบคลาวด์เป็นกระบวนการตรวจสอบและรับรองว่าระบบคลาวด์มีมาตรการความปลอดภัยที่เพียงพอและเป็นไปตามมาตรฐานที่กำหนด เพื่อป้องกันข้อมูลสำคัญจากการถูกโจมตี การรั่วไหล หรือการเข้าถึงโดยไม่ได้รับอนุญาต ซึ่งจากผลการประเมินระดับผลกระทบที่อาจเกิดขึ้นของสถาบันตามวัตถุประสงค์ด้านความมั่นคงปลอดภัยไซเบอร์ (Security Objectives) พบว่า ระดับผลกระทบอยู่ในระดับต่ำ ดังนั้น เพื่อให้สอดคล้องกับแนวทางการตรวจรับรองมาตรฐานฯ สถาบันจึงควรมีการประเมินตนเอง (Self-Assessment) ตามรูปแบบที่สถาบันกำหนดพร้อมแนบหลักฐาน และขออนุมัติไปยังผู้อำนวยการ โดยเก็บรักษาไว้ที่สถาบัน

ตารางที่ ๒ สรุประดับคุณลักษณะความมั่นคงปลอดภัยไซเบอร์และหัวข้อมาตรการควบคุมความมั่นคงปลอดภัยไซเบอร์ขั้นต่ำสำหรับข้อมูลหรือระบบสารสนเทศ

หัวข้อในการกำหนดมาตรการควบคุมความมั่นคงปลอดภัยไซเบอร์ขั้นต่ำสำหรับข้อมูลหรือระบบสารสนเทศ	**คุณลักษณะความมั่นคงปลอดภัยไซเบอร์ของข้อมูลหรือระบบสารสนเทศ**
ประมวลแนวทางปฏิบัติ	**ระดับต่ำ**
องค์ประกอบที่ ๑ แผนการตรวจสอบด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Audit Plan)	
องค์ประกอบที่ ๒ การประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Risk Assessment)	*
องค์ประกอบที่ ๓ แผนรับมือภัยคุกคามไซเบอร์ (Cybersecurity Risk Assessment)	*
กรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์	**ระดับต่ำ**
๑. การระบุความเสี่ยงที่อาจจะเกิดขึ้นแก่คอมพิวเตอร์ ข้อมูลคอมพิวเตอร์ ระบบคอมพิวเตอร์ ข้อมูลอื่นที่เกี่ยวข้องกับระบบคอมพิวเตอร์ ทรัพย์สิน และชีวิตร่างกายของบุคคล (Identify)	
๑.๑ การจัดการทรัพย์สิน (Asset Management)	
๑.๒ การประเมินความเสี่ยงและกลยุทธ์ในการจัดการความเสี่ยง (Risk Assessment and Risk Management Strategy)	*
๑.๓ การประเมินช่องโหว่และการทดสอบเจาะระบบ (Vulnerability Assessment and Penetration Testing)	*
๑.๔ การจัดการผู้ให้บริการภายนอก (Third Party Management)	
๒. มาตรการป้องกันความเสี่ยงที่อาจจะเกิดขึ้น (Protect)	
๒.๑ การควบคุมการเข้าถึง (Access Control)	*
๒.๒ การทำให้ระบบมีความแข็งแกร่ง (System Hardening)	*
๒.๓ การเชื่อมต่อระยะไกล (Remote Connection)	
๒.๔ สื่อเก็บข้อมูลแบบถอดได้ (Removable Storage Media)	
๒.๕ การสร้างความตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Awareness)	*
๒.๖ การแบ่งปันข้อมูล (Information Sharing)	
๓. มาตรการตรวจสอบและเฝ้าระวังภัยคุกคามทางไซเบอร์ (Detect)	
๓.๑ การตรวจสอบและเฝ้าระวังภัยคุกคามทางไซเบอร์ (Cyber Threat Detection and Monitoring)	
๔. มาตรการเผชิญเหตุเมื่อมีการตรวจพบภัยคุกคามทางไซเบอร์ (Respond)	
๔.๑ แผนการรับมือภัยคุกคามทางไซเบอร์ (Cybersecurity Incident Response Plan)	*
๔.๒ แผนการสื่อสารในภาวะวิกฤต (Crisis Communication Plan)	*

หัวข้อในการกำหนดมาตรการควบคุมความมั่นคงปลอดภัยไซเบอร์ขั้นต่ำสำหรับข้อมูลหรือระบบสารสนเทศ	คุณลักษณะความมั่นคงปลอดภัยไซเบอร์ของข้อมูลหรือระบบสารสนเทศ
๔.๓ การฝึกซ้อมความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Exercise)	*
๕. มาตรการรักษาและฟื้นฟูความเสียหายที่เกิดจากภัยคุกคามทางไซเบอร์ (Recover)	
๕.๑ การรักษาและฟื้นฟูความเสียหายที่เกิดจากภัยคุกคามทางไซเบอร์ (Cybersecurity Resilience and Recovery)	

ส่วนที่ ๒
ประมวลแนวทางปฏิบัติการรักษาความมั่นคงปลอดภัยไซเบอร์

แนวปฏิบัติ

๑. แผนการตรวจสอบด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

สถาบันต้องจัดให้มีการตรวจสอบด้านความมั่นคงปลอดภัยไซเบอร์โดยผู้ตรวจสอบด้านความมั่นคงปลอดภัยสารสนเทศทั้งโดยผู้ตรวจสอบภายใน หรือโดยผู้ตรวจสอบอิสระภายนอกอย่างน้อยปีละ ๑ ครั้ง โดยมีขอบเขตของการตรวจสอบอย่างน้อย ดังนี้

๑) กระบวนการจัดทำและผลการวิเคราะห์ผลกระทบธุรกิจ (Business Impact Analysis)
๒) บริการที่สำคัญที่สถาบันเป็นเจ้าของและใช้บริการ
๓) แนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

๒. การประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

สถาบันต้องกำหนดนโยบายการบริหารความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ ตามที่ระบุไว้ในนโยบายบริหารจัดการที่เกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์สำหรับสถาบัน ให้ครอบคลุมเรื่องโครงสร้างองค์กร และบทบาทหน้าที่ของผู้ที่เกี่ยวข้องในการบริหารความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ และต้องนำนโยบายดังกล่าวมาจัดทำระเบียบวิธีปฏิบัติและกระบวนการในการบริหารความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของสถาบัน โดยต้องจัดให้มีการประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์อย่างน้อยปีละ ๑ ครั้ง ต้องประกอบด้วยรายละเอียดอย่างน้อย ดังต่อไปนี้

๒.๑ การประเมินความเสี่ยง (Risk Assessment)

๑) การระบุความเสี่ยง (Risk Identification) ระบุถึงความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ซึ่งรวมถึงความเสี่ยงจากภัยคุกคามทางไซเบอร์ และช่องโหว่ต่าง ๆ โดยความเสี่ยงดังกล่าวอาจมีสาเหตุมาจากกระบวนการปฏิบัติงาน ระบบงาน บุคลากร หรือปัจจัยภายนอก

๒) การวิเคราะห์ความเสี่ยง (Risk Analysis) เข้าใจและวิเคราะห์ความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์เพื่อหาแนวทางในการจัดการความเสี่ยงที่เหมาะสม

๓) การประเมินค่าความเสี่ยง (Risk Evaluation) ประเมินถึงโอกาสที่ความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์จะเกิดขึ้น และผลกระทบต่อการปฏิบัติงานและการดำเนินธุรกิจรวมถึงกำหนดระดับความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ที่ยอมรับได้ (Risk Appetite)

๒.๒ การจัดการความเสี่ยง (Risk Treatment)

มีแนวทางจัดการ ควบคุม และป้องกันความเสี่ยงที่เหมาะสมสอดคล้องกับผลการประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์เพื่อให้ความเสี่ยงที่เหลืออยู่ (Residual Risk) อยู่ในระดับความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ที่ยอมรับได้

๒.๓ ติดตามและทบทวนความเสี่ยง (Risk Monitoring and Review)

มีกระบวนการที่มีประสิทธิภาพในการติดตาม และทบทวนความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ เพื่อให้อยู่ภายใต้ระดับความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ที่ยอมรับได้ที่กำหนดไว้

๒.๔ การรายงานความเสี่ยง (Risk Reporting)

รายงานระดับความเสี่ยงและผลการบริหารความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ต่อหัวหน้ากลุ่มงานสารสนเทศ หรือผู้บริหารเทคโนโลยีสารสนเทศ ระดับสูง ระดับกรม ที่ได้รับมอบหมาย เสนอต่อคณะทำงานบริหารความเสี่ยงและควบคุมภายในเพื่อรวบรวมและเสนอต่อผู้อำนวยการพิจารณาต่อไป

ทั้งนี้ ต้องทบทวนระเบียบวิธีปฏิบัติและกระบวนการบริหารความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ อย่างน้อยปีละ ๑ ครั้ง และทุกครั้งที่มีการเปลี่ยนแปลงอย่างมีนัยสำคัญ เช่น กรณีที่มีการเปลี่ยนแปลงของระบบความมั่นคงปลอดภัยไซเบอร์ ความเสี่ยง มาตรฐานสากล อย่างมีนัยสำคัญ เป็นต้น

๓. แผนการรับมือภัยคุกคามทางไซเบอร์

สถาบันต้องดำเนินการจัดทำแผนการรับมือภัยคุกคามทางไซเบอร์ โดยดำเนินการดังต่อไปนี้

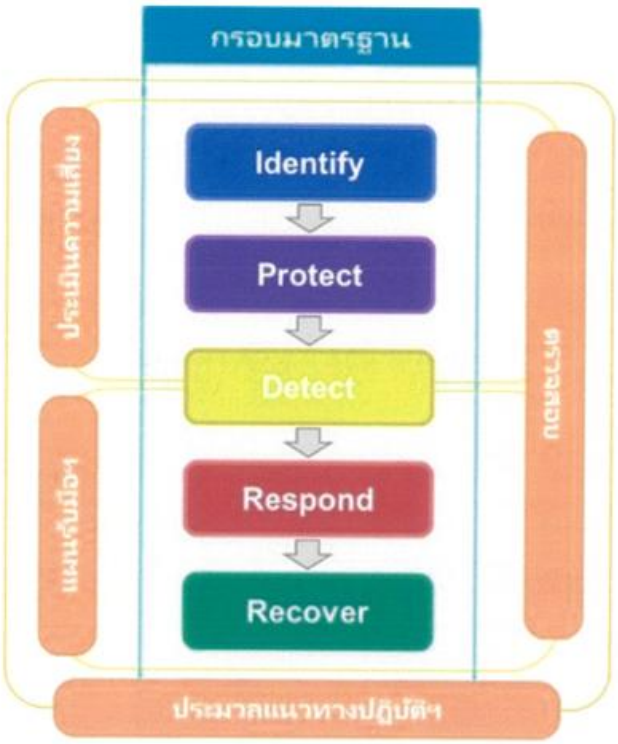
๓.๑ จัดทำแผนการรับมือภัยคุกคามทางไซเบอร์ (Cybersecurity Incident Response Plan)

๓.๒ ตรวจสอบแผนการรับมือภัยคุกคามทางไซเบอร์ได้รับการสื่อสารอย่างมีประสิทธิผลไปยังบุคลากร ที่เกี่ยวข้อง

๓.๓ ทบทวนแผนการรับมือภัยคุกคามทางไซเบอร์อย่างน้อยปีละ ๑ ครั้ง

๓.๔ ทบทวนแผนการรับมือภัยคุกคามทางไซเบอร์ เมื่อมีการเปลี่ยนแปลงอย่างมีนัยสำคัญ ในสภาพแวดล้อมการปฏิบัติการทางไซเบอร์ของบริการที่สำคัญของสถาบัน หรือข้อกำหนดในการตอบสนองต่อเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์

๓.๕ ฝึกซ้อมแผนการรับมือภัยคุกคามทางไซเบอร์อย่างน้อยปีละ ๑ ครั้ง



รูปที่ ๑ ประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

๔ การรายงานสถานการณ์เกี่ยวกับด้านความมั่นคงปลอดภัยไซเบอร์

สถาบันต้องรายงานสถานการณ์เกี่ยวกับด้านความมั่นคงปลอดภัยไซเบอร์มายังคณะอนุกรรมการอย่างน้อยดังนี้

๔.๑ แนวนโยบายหรือแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยไซเบอร์

๔.๒ เหตุการณ์ภัยคุกคามทางไซเบอร์ (Cyber Security Incident) ที่ตรวจพบ และผลดำเนินการในการตรวจสอบเหตุการณ์ภัยคุกคามทางไซเบอร์ (Cyber Security Incident) (ถ้ามี)

๔.๓ การดำเนินการเพื่อทำให้ระบบความมั่นคงปลอดภัยมีความแข็งแกร่ง (Hardening)

๔.๔ การดำเนินการทางกฎหมายที่เกี่ยวข้องในการตอบสนองต่อเหตุการณ์ภัยคุกคามทางไซเบอร์ (Cyber Security Incident)

๔.๕ การพัฒนาด้านบุคลากรด้านความมั่นคงปลอดภัยไซเบอร์

๔.๖ การรายงานปัญหาและอุปสรรคที่เกิดขึ้นในด้านความมั่นคงปลอดภัยไซเบอร์ เพื่อหาแนวทางในการแก้ไขปัญหาที่เกิดขึ้น

ส่วนที่ ๓
กรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

หัวข้อที่ ๑ การระบุความเสี่ยงที่อาจจะเกิดขึ้นแก่คอมพิวเตอร์ ข้อมูลคอมพิวเตอร์ ระบบคอมพิวเตอร์ ข้อมูลอื่นที่เกี่ยวข้องกับระบบคอมพิวเตอร์ ทรัพย์สินและชีวิตร่างกายของบุคคล (Identify)

๑.๑ การจัดการทรัพย์สิน (Asset Management)

การจัดเก็บรายละเอียดข้อมูลของอุปกรณ์ด้านเทคโนโลยีสารสนเทศของฮาร์ดแวร์ (Hardware) และซอฟต์แวร์ (Software) ทั้งหมดของระบบเพื่อใช้ในการวางแผนและการบริหารด้านความมั่นคงปลอดภัยทางไซเบอร์

๑.๑.๑ สถาบันต้องมีทะเบียนทรัพย์สิน (Inventory) ที่ระบุทรัพย์สินด้านเทคโนโลยีสารสนเทศของฮาร์ดแวร์ (Hardware) และซอฟต์แวร์ (Software) และดูแลรักษาทะเบียนทรัพย์สินให้เป็นปัจจุบัน โดยทะเบียนทรัพย์สินแต่ละประเภทต้องมีข้อมูลอย่างน้อย ดังนี้

๑) ชื่อ/คำอธิบายของทรัพย์สิน
๒) ประเภทของอุปกรณ์/ยี่ห้อ
๓) ฟังก์ชันที่สำคัญของทรัพย์สิน
๔) ชื่อระบบปฏิบัติการ (Operation System) และเวอร์ชัน
๕) การระบุและจัดลำดับความสำคัญของทรัพย์สิน
๖) เจ้าของและ/หรือผู้ดำเนินการของทรัพย์สิน
๗) ตำแหน่งทางกายภาพของทรัพย์สินบนระบบหรือเครือข่ายภายในและ/หรือภายนอก
๘) การขึ้นต่อกันของทรัพย์สิน

๑.๑.๒ สถาบันต้องมีทะเบียนทรัพย์สินข้อมูลที่ระบุข้อมูลที่เก็บไว้ภายในระบบสารสนเทศ

๑.๑.๓ สถาบันต้องระบุขอบเขตเครือข่ายของบริการที่สำคัญของสถาบันและระบบคอมพิวเตอร์ที่เชื่อมต่อโดยตรงและมีนัยสำคัญ (Direct and Significant Interface)

๑.๑.๔ สถาบันต้องมีการตรวจสอบทะเบียนทรัพย์สินอย่างน้อยปีละ ๑ ครั้ง หากมีการเปลี่ยนแปลงใด ๆ กับทรัพย์สินของบริการที่สำคัญของสถาบันให้ปรับปรุงทะเบียนทรัพย์สินดังกล่าวด้วย

๑.๑.๕ สถาบันต้องดำเนินการประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของบริการที่สำคัญของสถาบันซึ่งรวมถึงรายการทั้งหมดที่ระบุไว้ในทะเบียนทรัพย์ใน ข้อ ๑.๑.๑ อย่างน้อยปีละ ๑ ครั้ง

๑.๑.๖ สถาบันต้องดำเนินการจัดทำแผนผังเครือข่าย (Network Diagram) ของสถาบันและปรับปรุงให้เป็นปัจจุบัน

๑.๒ การประเมินความเสี่ยงและกลยุทธ์ในการจัดการความเสี่ยง (Risk Assessment and Risk Management strategy)

การประเมินความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์เพื่อเป็นการเตรียมความพร้อมในการรับมือเหตุการณ์ด้านความมั่นคงปลอดภัยไซเบอร์ที่อาจจะเกิดขึ้นกับสถาบัน พร้อมทั้งหาแนวทางในการรับมือเพื่อลดความเสียหายที่จะเกิดกับสถาบัน

๑.๒.๑ สถาบันต้องประเมินความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์อย่างน้อยปีละ ๑ ครั้ง โดยต้องมีข้อมูลอย่างน้อย ดังนี้

๑) กำหนดหน้าที่และความรับผิดชอบในการบริหารและจัดการความเสี่ยง

๒) ระบุความเสี่ยงที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศ (IT-Related Risk)

๓) ประเมินความเสี่ยงที่ครอบคลุมถึงโอกาสหรือความถี่ที่จะเกิดความเสี่ยงและผลกระทบที่จะเกิดขึ้น เพื่อจัดลำดับความสำคัญในการบริหารจัดการความเสี่ยง

๔) กำหนดวิธีการหรือเครื่องมือในการบริหาร และจัดการความเสี่ยงให้อยู่ในระดับที่องค์กรยอมรับได้

๑.๒.๒ สถาบันต้องปรับปรุงทะเบียนความเสี่ยงทุกครั้งหลังการประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ ทะเบียนความเสี่ยงต้องจัดทำเอกสาร โดยมีรายละเอียดอย่างน้อยดังต่อไปนี้

๑) วันที่ระบุความเสี่ยง (Date the Risk is Identified)

๒) คำอธิบายของความเสี่ยง (Description of the Risk)

๓) โอกาสที่จะเกิดขึ้น (Likelihood of Occurrence)

๔) ความรุนแรงของเหตุการณ์ (Severity of the Occurrence)

๕) การจัดการความเสี่ยง (Risk Treatment)

๖) เจ้าของความเสี่ยง (Risk Owner)

๗) สถานะของการจัดการความเสี่ยง (Status of Risk Treatment)

๘) ความเสี่ยงที่เหลือ (Residual Risk)

หัวข้อที่ ๒ มาตรการป้องกันความเสี่ยงที่อาจจะเกิดขึ้น (Protect)

๒.๑ การควบคุมการเข้าถึง (Access Control)

การอนุญาต การกำหนดสิทธิ์หรือการมอบอำนาจให้ผู้ใช้งาน เข้าถึงหรือใช้งานเครือข่ายหรือระบบสารสนเทศทั้งทางอิเล็กทรอนิกส์และทางกายภาพ รวมทั้งการอนุญาตเช่นว่านั้นสำหรับบุคคลภายนอกในการเข้าถึงบริการที่สำคัญของสถาบัน

๒.๑.๑ สถาบันต้องควบคุมการเข้าถึงข้อมูลและอุปกรณ์ในการประมวลผลข้อมูลโดยคำนึงถึง การใช้งานและความมั่นคงปลอดภัย อย่างน้อยดังนี้

๑) การควบคุมการเข้าถึงเครือข่าย (Network Access Control)

๒) การควบคุมการเข้าถึงระบบปฏิบัติการ (Operating System Access Control)

๓) การควบคุมการเข้าถึงเครื่องคอมพิวเตอร์แม่ข่ายและอุปกรณ์ระบบเครือข่าย

๔) การควบคุมการเข้าถึงระบบงานและแอปพลิเคชัน

๕) การบริหารจัดการการเข้าถึงด้านระบบเทคโนโลยีสารสนเทศของผู้ใช้งาน

๒.๑.๒ สถาบันต้องกำหนดกฎเกณฑ์เกี่ยวกับการอนุญาตให้เข้าถึง โดยกำหนดตามนโยบายที่เกี่ยวข้องกับการอนุญาตการกำหนดสิทธิ์หรือการมอบอำนาจของสถาบัน ให้สอดคล้องกับหน้าที่ความรับผิดชอบของเจ้าหน้าที่

๒.๑.๓ สถาบันต้องกำหนดเกี่ยวกับประเภทของข้อมูล ลำดับความสำคัญหรือลำดับชั้นความลับของข้อมูล รวมทั้งระดับชั้นการเข้าถึง เวลาที่ได้เข้าถึงและช่องทางการเข้าถึง

๒.๑.๔ สถาบันต้องตรวจสอบให้แน่ใจว่าการเข้าถึงอินเทอร์เฟซ (Interface) ของบริการที่สำคัญของสถาบัน (เช่น USB, พอร์ตอนุกรม) และการเข้าถึงทางลอจิกัล (Logical) มีการกำกับดูแลโดยกลุ่มงานสารสนเทศหรือผู้รับจ้างของสถาบันเท่านั้น

๒.๑.๕ สถาบันต้องเก็บรักษาบันทึกของการเข้าถึงทั้งหมด (Logs of All Access) และความพยายามทั้งหมดในการเข้าถึงบริการที่สำคัญของสถาบันและตรวจสอบบันทึกเหล่านี้เพื่อหากิจกรรมที่ผิดปกติเป็นประจำ

๒.๑.๖ ในการเข้าถึงระบบสารสนเทศของสถาบันต้องมีการเข้ารหัส Transaction ที่มีความปลอดภัย เช่น Secure Socket Layer (SSL) หรือ Transport Layer Security (TLS) เป็นต้น โดยต้องใช้ใบรับรอง (Certificate) ที่มีความปลอดภัย

๒.๒ การทำให้ระบบมีความแข็งแกร่ง (System Hardening)

๒.๒.๑ สถาบันต้องสร้างมาตรฐานการกำหนดค่าขั้นต่ำด้านความมั่นคงปลอดภัย (Security Baseline Configuration Standards) สำหรับระบบปฏิบัติการ แอปพลิเคชัน และอุปกรณ์เครือข่ายทั้งหมด ของบริการที่สำคัญของสถาบัน

๒.๒.๒ สถาบันต้องจัดทำมาตรฐานการกำหนดค่าขั้นต่ำด้านความมั่นคงปลอดภัย (Security Baseline Configuration Standards) ต้องมีหลักการรักษาความมั่นคงปลอดภัย อย่างน้อยดังต่อไปนี้

๑) สิทธิพิเศษในการเข้าถึงน้อยที่สุด (Least Access Privilege)

๒) การแบ่งแยกหน้าที่ (Separation of Duties)

๓) การบังคับใช้นโยบายความซับซ้อนของรหัสผ่าน

๔) การลบบัญชีที่ไม่ได้ใช้

๕) การลบบริการและแอปพลิเคชันที่ไม่จำเป็น เช่น การลบคอมไพเลอร์ (Removal of Compiler) และแอปพลิเคชันสนับสนุนผู้ให้บริการภายนอก (Vendor Support Application)

๖) การปิดพอร์ตเครือข่ายที่ไม่ได้ใช้งาน

๗) การป้องกันมัลแวร์ (Malware)

๘) การปรับปรุงซอฟต์แวร์และแพตช์ (Patch) ความมั่นคงปลอดภัยของระบบอย่างทันการณ์ และเหมาะสม

๒.๒.๓ สถาบันต้องตรวจสอบให้แน่ใจว่ามีการใช้มาตรฐานการกำหนดค่าขั้นต่ำด้านความมั่นคงปลอดภัย (Security Baseline Configuration Standards) ตามที่ระบุไว้ก่อนที่จะมีทรัพย์สินใด ๆ เชื่อมต่อ หรือเมื่อมีการเปลี่ยนแปลงหรือปรับปรุงบริการที่สำคัญของสถาบัน

๒.๒.๔ สถาบันต้องตรวจสอบมาตรฐานการกำหนดค่าขั้นต่ำด้านความมั่นคงปลอดภัย (Security Baseline Configuration Standard) ของบริการที่สำคัญของสถาบันอย่างน้อยปีละ ๑ ครั้ง เพื่อให้แน่ใจว่ามาตรฐานเหล่านี้ยังคงมีประสิทธิภาพต่อภัยคุกคามทางไซเบอร์

๒.๒.๕ สถาบันต้องจัดทำกระบวนการจัดการเปลี่ยนแปลง (Change Management Process) เพื่ออนุญาต และตรวจสอบความถูกต้องของการเปลี่ยนแปลงระบบทั้งหมดที่มีต่อบริการที่สำคัญของสถาบัน

๒.๓ การสร้างความตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Awareness)

๒.๓.๑ สถาบันต้องเผยแพร่ ประชาสัมพันธ์ เกี่ยวกับแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศและสร้างความตระหนักถึงความสำคัญของการปฏิบัติให้กับผู้ใช้งาน ในลักษณะเกร็ดความรู้ หรือข้อระวังในรูปแบบที่สามารถเข้าใจและนำไปปฏิบัติได้ง่าย

๒.๓.๒ สถาบันต้องจัดทำ ปรับปรุง คู่มือการใช้งานระบบสารสนเทศให้เป็นปัจจุบัน และมีการเผยแพร่ผ่านช่องทางที่เหมาะสมของสถาบัน

๒.๓.๓ สถาบันต้องจัดฝึกอบรมการใช้งานระบบสารสนเทศของสถาบันอย่างน้อยปีละ ๑ ครั้ง หรือเมื่อมีการปรับปรุง และเปลี่ยนแปลงการใช้งานของระบบสารสนเทศ

๒.๓.๔ สถาบันต้องสร้างความตระหนัก (Awareness Program) เรื่องการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ ความเสี่ยงด้านเทคโนโลยีสารสนเทศ การใช้งานระบบอย่างปลอดภัย ให้แก่บุคลากรทุกระดับ

๒.๓.๕ สถาบันควรจัดให้มีการฝึกอบรม และพัฒนาความรู้ความเชี่ยวชาญให้ครอบคลุม และเพียงพอต่อการปฏิบัติงานด้านการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ กับเจ้าหน้าที่ที่ดูแลระบบสารสนเทศ

หัวข้อที่ ๓ มาตรการตรวจสอบและเฝ้าระวังภัยคุกคามทางไซเบอร์ (Detect)

การตรวจสอบและเฝ้าระวังภัยคุกคามทางไซเบอร์ (Cyber Threat Detection and Monitoring) การตรวจสอบการกระทำหรือการดำเนินการใด ๆ โดยมิชอบ โดยใช้เครื่องคอมพิวเตอร์ หรือระบบคอมพิวเตอร์ หรือโปรแกรมที่ไม่พึงประสงค์ ซึ่งมีจุดมุ่งหมายให้เกิดการประทุษร้ายต่อระบบคอมพิวเตอร์ ข้อมูลคอมพิวเตอร์ หรือข้อมูลอื่นที่เกี่ยวข้อง และเป็นภัยอันตรายที่ใกล้จะถึงที่จะก่อให้เกิดความเสียหายหรือส่งผลกระทบต่อการทำงานของเครื่องคอมพิวเตอร์ ระบบคอมพิวเตอร์ หรือข้อมูลที่เกี่ยวข้อง เพื่อให้อยู่ภายใต้ระดับความเสี่ยงด้านเทคโนโลยีสารสนเทศที่ยอมรับได้ที่กำหนดไว้ โดยสถาบันต้องมีกระบวนการในการตรวจสอบและเฝ้าระวังภัยคุกคามทางไซเบอร์ ดังต่อไปนี้

๓.๑ การตรวจจับเหตุการณ์ผิดปกติที่กระทบต่อความมั่นคงปลอดภัยทางไซเบอร์

๓.๒ การจัดประเภทและวิเคราะห์เหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ที่ตรวจพบ

๓.๓ การระบุว่ามีภัยคุกคามทางไซเบอร์หรือเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ที่เกี่ยวข้องกับบริการที่สำคัญของสถาบัน

๓.๔ ต้องดำเนินการทบทวนกลไก และกระบวนการเฝ้าระวังภัยคุกคามทางไซเบอร์อย่างน้อยปีละ ๑ ครั้ง เพื่อให้แน่ใจว่ากลไก และกระบวนการต่าง ๆ ยังคงมีประสิทธิภาพ

หัวข้อที่ ๔ มาตรการเผชิญเหตุเมื่อมีการตรวจพบภัยคุกคามทางไซเบอร์ (Respond)

มาตรการเผชิญเหตุเมื่อมีการตรวจพบภัยคุกคามทางไซเบอร์ (Respond) ซึ่งมีแผนเกี่ยวข้องกับการตรวจพบภัยคุกคามทางไซเบอร์ จำนวน ๒ แผน ดังนี้

๔.๑ แผนการรับมือภัยคุกคามทางไซเบอร์ (Cybersecurity Incident Response Plan) สถาบันต้องมีการจัดทำ สื่อสาร ฝึกซ้อม ทบทวน และปรับปรุง แผนการรับมือภัยคุกคามทางไซเบอร์ ตามที่ระบุไว้ในประมวลแนวทางปฏิบัติการรักษาความมั่นคงปลอดภัยไซเบอร์อย่างน้อยปีละ ๑ ครั้ง เพื่อให้แน่ใจว่าแผนการรับมือภัยคุกคามทางไซเบอร์สามารถดำเนินการได้อย่างมีประสิทธิภาพ และประสิทธิผล

๔.๒ แผนการสื่อสารในภาวะวิกฤต (Crisis Communication Plan)

๔.๒.๑ สถาบันต้องจัดทำแผนการสื่อสารในภาวะวิกฤตเพื่อตอบสนองต่อวิกฤตที่เกิดจากเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์

๔.๒.๒ สถาบันต้องตรวจสอบแผนการสื่อสารในภาวะวิกฤต

๑) จัดตั้งทีมสื่อสารในภาวะวิกฤตเพื่อเปิดใช้งานในช่วงวิกฤต

๒) ระบุสถานการณ์จำลองเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ ที่เป็นไปได้ และแผนการดำเนินการที่เกี่ยวข้อง

๓) ระบุกลุ่มเป้าหมาย และผู้มีส่วนได้ส่วนเสียสำหรับสถานการณ์จำลองเหตุการณ์ ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์แต่ละประเภท

๔) ระบุโฆษกหลัก และผู้เชี่ยวชาญด้านเทคนิคที่จะเป็นตัวแทนขององค์กรเมื่อกล่าวแถลงกับสื่อมวลชน

๕) ระบุแพลตฟอร์ม/ช่องทางการเผยแพร่ที่เหมาะสม เช่น สื่อดั้งเดิม และโซเชียลมีเดีย สำหรับการเผยแพร่ข้อมูล

๔.๒.๓ สถาบันต้องตรวจสอบแผนการสื่อสารในภาวะวิกฤต รวมถึงการประสาน งานระหว่างทุกฝ่ายที่ได้รับผลกระทบเพื่อให้แน่ใจว่ามีการตอบสนองที่ประสานกันและสอดคล้องกันในช่วงวิกฤต

๔.๒.๔ สถาบันต้องดำเนินการฝึกซ้อมแผนการสื่อสารในภาวะวิกฤตอย่างน้อยปีละ ๑ ครั้ง เพื่อให้แน่ใจว่าสามารถสื่อสารและเผยแพร่ข้อมูลได้อย่างทันท่วงทีและมีประสิทธิผล ในช่วงวิกฤตอันเนื่องมาจากเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์

หัวข้อที่ ๕ มาตรการรักษาและฟื้นฟูความเสียหายที่เกิดจากภัยคุกคามทางไซเบอร์ (Cybersecurity Resilience and Recovery)

การรักษาและฟื้นฟูความเสียหายที่เกิดจากภัยคุกคามทางไซเบอร์ (Cybersecurity Resilience and Recovery) เมื่อมีภัยคุกคามทางไซเบอร์เกิดขึ้น หรือเมื่อสถาบันได้รับแจ้งเตือนการเกิดภัยคุกคามทางไซเบอร์ สถาบันควรกำหนดแนวทางการดำเนินมาตรการเพื่อระงับภัยคุกคามทางไซเบอร์ การปราบปรามภัยคุกคามทางไซเบอร์ และการฟื้นฟูระบบงานที่ได้รับผลกระทบ (Containment, eradication and recovery) โดยการดำเนินการดังกล่าว ควรกำหนดให้สอดคล้องกับความรุนแรง และระดับของภัยคุกคามทางไซเบอร์ แต่ละระดับจนกระทั่งสามารถกู้คืนทรัพย์สินสำคัญทางสารสนเทศให้กลับมาดำเนินงานหรือให้บริการได้ตามปกติ ซึ่งการดำเนินการในขั้นตอนนี้ อาจต้องกระทำควบคู่ไปกับการตรวจจับและวิเคราะห์ภัยคุกคามทางไซเบอร์ ที่อาจมีการลุกลามหรือทวีความรุนแรงมากขึ้น

๕.๑ สถาบันต้องจัดทำแผนความต่อเนื่องทางธุรกิจ (Business Continuity Plan : BCP)

เพื่อให้แน่ใจว่า บริการที่สำคัญของสถาบัน สามารถให้บริการที่จำเป็นต่อไปได้ในกรณีที่เกิดการหยุดชะงักเนื่องจากเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ เพื่อให้สามารถใช้ปฏิบัติงานได้จริง เพื่อพิจารณาความสอดคล้องกับแผนของสถาบัน เช่น ความสอดคล้องกันของขอบเขตคำนิยามและการกำหนดระยะเวลาที่สำคัญ เช่น Maximum Tolerable Period of Disruption (MTPD), Recovery Time Objective (RTO) และ Recovery Point Objective (RPO) เป็นต้น โดยมีรายละเอียดอย่างน้อยดังนี้

๕.๑.๑ จัดลำดับความสำคัญของความเสี่ยงด้านความมั่นคงปลอดภัยทางไซเบอร์และสารสนเทศ โดยต้องพิจารณาจากปัจจัยที่สำคัญ เช่น ผลกระทบของการหยุดชะงัก ระยะเวลาที่ยอมรับได้ของการหยุดชะงัก ลำดับความสำคัญในการกู้คืนระบบ

๕.๑.๒ จัดทำแผนกู้คืนภาวะวิกฤต สำหรับกระบวนการดำเนินงานของสถาบันที่ใช้ทรัพย์สินสารสนเทศที่มีระดับการป้องกันความมั่นคงปลอดภัย “สูง” หรือ “สูงสุด” เพื่อให้มั่นใจว่าสามารถดำเนินงานได้ อย่างต่อเนื่อง มีการควบคุมดูแลการแก้ไขและกู้คืนระบบ เมื่อเกิดเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยทางไซเบอร์และสารสนเทศ

๕.๒ สถาบันต้องตรวจสอบให้แน่ใจว่ามีการฝึกซ้อมแผนความต่อเนื่องธุรกิจ

อย่างน้อยปีละ ๑ ครั้ง เพื่อประเมินประสิทธิภาพของแผนความต่อเนื่องธุรกิจ (Business Continuity Plan: BCP) ต่อภัยคุกคามทางไซเบอร์และเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์

๕.๓ ในกรณีตรวจพบภัยคุกคามทางไซเบอร์ (Cyber Security Incident)

สถาบันต้องจัดทำรายงานภัยคุกคามทางไซเบอร์ (Incident Report) โดยรายงานความคืบหน้าของการดำเนินการ ให้ผู้บังคับบัญชาและผู้บริหารเทคโนโลยีสารสนเทศระดับสูง ระดับกรมทราบทุกระยะ

เอกสารอ้างอิง

- พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒
- ประกาศคณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง การกำหนดหลักเกณฑ์ ลักษณะสถาบันที่มีภารกิจหรือให้บริการเป็นสถาบันโครงสร้างพื้นฐานสำคัญทางสารสนเทศ และการมอบหมายการควบคุมและกำกับดูแล พ.ศ. ๒๕๖๔
- ประกาศคณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง ประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ สำหรับหน่วยงานของรัฐและสถาบันโครงสร้างพื้นฐานสำคัญทางสารสนเทศ พ.ศ. ๒๕๖๔
- (ร่าง) นโยบายบริหารจัดการที่เกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์สำหรับหน่วยงานของรัฐและสถาบันโครงสร้างพื้นฐานสำคัญทางสารสนเทศ
- (ร่าง) ประกาศสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.) เรื่อง การประเมินความเสี่ยงและกลยุทธ์ในการจัดการความเสี่ยง สำหรับหน่วยงานของรัฐและสถาบันโครงสร้างพื้นฐานสำคัญทางสารสนเทศ พ.ศ.๒๕๖๔ (NIST ๘๐๐-๓๙)
- (ร่าง) ประกาศสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.) เรื่อง การประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ สำหรับหน่วยงานของรัฐ และสถาบันโครงสร้างพื้นฐานสำคัญทางสารสนเทศ พ.ศ.๒๕๖๔ (NIST ๘๐๐-๓๐)
- (ร่าง) ประกาศสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.) เรื่อง กรอบการบริหารความเสี่ยงด้านไซเบอร์ สำหรับหน่วยงานของรัฐและสถาบันโครงสร้างพื้นฐานสำคัญทางสารสนเทศ พ.ศ.๒๕๖๔ (NIST ๘๐๐-๓๗)

ภาคผนวก

แผนบริหารความต่อเนื่องทางธุรกิจ ด้านเทคโนโลยีสารสนเทศ (Business Continuity Plan: BCP ด้าน IT) ฉบับทบทวน พ.ศ. ๒๕๖๙



itd
International Institute for Trade and Development

ได้รับอนุมัติเมื่อ: ๒๕๖๙
เวอร์ชัน 2.00

การอนุมัติแผนบริหารความต่อเนื่องทางธุรกิจ

แผนบริหารความต่อเนื่องทางธุรกิจนี้สรุปหน้าที่ทางธุรกิจที่สำคัญของบริการด้านสารสนเทศ (Business Continuity Plan: BCP ด้าน IT) ฉบับทบทวน พ.ศ.๒๕๖๙ และทรัพยากรที่จำเป็นเพื่อดำเนินการต่อหน้าที่ทางธุรกิจที่สำคัญที่ระบุหลังจากการหยุดชะงัก

เอกสารนี้ได้รับการรับรองเป็นแผนที่ได้รับการอนุมัติของสถาบันที่จะต้องปฏิบัติตามในกรณีที่เกิดการหยุดชะงักดังกล่าว

อนุมัติโดย

_____

(นายวิมล ปั้นคง)

รองผู้อำนวยการ (วิชาการ)

ผู้บริหารเทคโนโลยีสารสนเทศระดับกรม

สถาบันระหว่างประเทศเพื่อการค้าและการพัฒนา (องค์การมหาชน)

วันที่อนุญาต: .....

๑. บทนำ

๑.๑ ความเป็นมา

สถาบันระหว่างประเทศเพื่อการค้าและการพัฒนา (องค์การมหาชน) ได้จัดทำและปรับปรุงแผนบริหารความต่อเนื่องทางธุรกิจด้านเทคโนโลยีสารสนเทศ (Business Continuity Plan: BCP ด้าน IT) ฉบับทบทวน พ.ศ. ๒๕๖๙ ขึ้น เพื่อกำหนดกรอบนโยบาย หลักเกณฑ์และมาตรการที่ต้องถือปฏิบัติ ขั้นตอนการดำเนินงานเชิงปฏิบัติการ ตลอดจนการจัดสรรและบริหารจัดการทรัพยากรที่จำเป็นอย่างเป็นระบบ สำหรับใช้ในการตอบสนอง เผชิญเหตุ และบริหารจัดการภาวะวิกฤตเมื่อเกิดเหตุการณ์ฉุกเฉิน ภัยพิบัติ หรือเหตุภัยคุกคามทางไซเบอร์ขั้นวิกฤต (Cybersecurity Incident) ที่ส่งผลกระทบ หรือมีศักยภาพที่จะก่อให้เกิดการหยุดชะงักต่อการทำงานของระบบสารสนเทศ โครงสร้างพื้นฐานดิจิทัล และบริการทางอิเล็กทรอนิกส์ที่สำคัญของสถาบัน

แผนบริหารความต่อเนื่องทางธุรกิจฉบับนี้ มุ่งเน้นการคุ้มครองและกู้คืนระบบงานหลักที่ให้บริการทางอิเล็กทรอนิกส์ของสถาบัน ทั้ง ๖ ระบบ ได้แก่ ระบบเว็บไซต์สถาบัน (itd.or.th), ระบบเว็บไซต์ BCG CONNEX (BCGconnex.com) ระบบบริหารจัดการสำนักงาน (e-Office) ระบบบริหารจัดการงบประมาณและการเงิน (e-Budget) ระบบ Prompt Pass และระบบบริหารจัดการบุคลากร (Humansoft) ซึ่งดำเนินงานบนโครงสร้างพื้นฐานคลาวด์ภาครัฐ (GDCC) และผู้ให้บริการคลาวด์ภายนอก ทั้งนี้ เพื่อให้สถาบันสามารถกู้คืนระบบและรักษาความต่อเนื่องในการให้บริการแก่ภาคธุรกิจ บุคลากรภาครัฐ และสาธารณชนได้อย่างมีประสิทธิภาพ ทันท่วงที ภายในระยะเวลาเป้าหมายที่ยอมรับได้ (RTO/RPO/MTD) ป้องกันความเสียหายต่อข้อมูลวิกฤต ลดผลกระทบต่อชื่อเสียงและความน่าเชื่อถือ ตลอดจนสอดรับกับข้อกำหนดตามพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ อย่างยั่งยืน

๑.๒ วัตถุประสงค์

๑) เพื่อคุ้มครองความปลอดภัยของบุคลากร และปกป้องสินทรัพย์ด้านเทคโนโลยีสารสนเทศของสถาบัน

๒) เพื่อใช้วางมาตรการเชิงป้องกันและรับมือในภาวะฉุกเฉิน ป้องกันการสูญเสียและความปลอดภัยของบุคลากรผู้ปฏิบัติงาน ควบคู่ไปกับการปกป้องความเสียหายต่อสินทรัพย์ทางเทคโนโลยี โครงสร้างพื้นฐานเครือข่าย เครื่องคอมพิวเตอร์ ตลอดจนฐานข้อมูลวิกฤตของสถาบัน เพื่อลดผลกระทบด้านลบที่อาจเกิดขึ้นต่อการให้บริการทางอิเล็กทรอนิกส์ให้เหลือน้อยที่สุด

๓) เพื่อจัดทำกระบวนการตอบสนองและกู้คืนระบบอย่างเป็นระบบและมีโครงสร้างที่ชัดเจน

๔) เพื่อสร้างและกำหนดขั้นตอนการปฏิบัติงานมาตรฐาน (SOP) ในการบริหารจัดการภาวะวิกฤต ที่ช่วยให้สถาบันสามารถรับมือ เผชิญเหตุ และตอบสนองต่อการหยุดชะงักของระบบสารสนเทศ ทั้งที่คาดหมายได้และไม่คาดหมายได้อย่างมีประสิทธิผล สามารถเปิดใช้ระบบสำรองหรือระบบคลาวด์ (GDCC/Cloud Services) ตลอดจนการสลับไปใช้วิธีการทำงานสำรองด้วยมือ (Manual Operation) ได้อย่างทันท่วงทีภายในระยะเวลาเป้าหมายที่กำหนด (RTO/RPO/MTD)

๕) เพื่อลดผลกระทบจากการหยุดชะงักของกระบวนงานวิกฤต และสร้างความเชื่อมั่นแก่ผู้มีส่วนได้ส่วนเสีย:

๖) เพื่อลดความเสี่ยงและบรรเทาความเสียหายจากการหยุดชะงักของบริการทางอิเล็กทรอนิกส์สำคัญทั้ง ๖ ระบบ ได้แก่ ระบบเว็บไซต์สถาบัน ระบบเว็บไซต์ BCG CONNEX ระบบสารบรรณอิเล็กทรอนิกส์ (e-Office) ระบบบริหารจัดการงบประมาณ (e-Budget) ระบบ Prompt Pass และระบบบริหารบุคลากร

(Humansoft) อันเป็นการปกป้องผลประโยชน์ สิทธิ์ในข้อมูล และลดผลกระทบต่อผู้รับบริการ ภาคธุรกิจ บุคลากรภาครัฐ ประชาชนผู้มาติดต่อ เจ้าหน้าที่ และผู้มีส่วนได้ส่วนเสียทุกภาคส่วน

๗) เพื่อยกระดับมาตรการความต่อเนื่องทางธุรกิจด้านสารสนเทศของสถาบันให้ถูกต้อง สอดคล้องกับข้อกำหนดของพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ อย่างยั่งยืน

๑.๓ ขอบเขตของแผน

แผนบริหารความต่อเนื่องทางธุรกิจฉบับนี้ มีขอบเขตการบังคับใช้ครอบคลุมกรณีที่เกิดการหยุดชะงักของบริการ อันเนื่องมาจากการสูญเสียสภาพการใช้งานเป็นเวลานาน หรือการถูกปฏิเสธการเข้าถึงโครงสร้างพื้นฐาน ระบบเทคโนโลยีสารสนเทศ และสถานที่ตั้งของระบบให้บริการทางอิเล็กทรอนิกส์ของสถาบัน

โดยแผนฉบับนี้ให้ครอบคลุมถึงทุกกิจกรรม กระบวนงาน เทคโนโลยี และทรัพยากรที่จำเป็นทั้งหมด เพื่อสร้างความแน่ใจว่า หน้าที่และภารกิจสำคัญของบริการทางอิเล็กทรอนิกส์ของสถาบัน จะสามารถดำเนินไปได้อย่างต่อเนื่องในภาวะที่การดำเนินงานตามปกติเกิดการหยุดชะงัก หรือเผชิญกับภัยคุกคามที่อาจส่งผลกระทบก่อให้เกิดการหยุดชะงักขึ้น

๑.๔ สมมติฐานของแผน

การจัดทำและขับเคลื่อนแผนบริหารความต่อเนื่องทางธุรกิจด้านเทคโนโลยีสารสนเทศฉบับนี้ ตั้งอยู่บนสมมติฐานสำคัญอันเป็นส่วนหนึ่งของกระบวนการวางแผน ดังต่อไปนี้

๑) ฐานการพิจารณาและการกำกับดูแล สมมติฐานของแผนฉบับนี้ ตั้งอยู่บนพื้นฐานของการพิจารณา การคาดการณ์ และการประเมินบริบทความเสี่ยงอย่างสมเหตุสมผล ซึ่งสอดคล้องและเป็นไปตามกรอบการกำกับดูแล นโยบายการบริหารความต่อเนื่องทางธุรกิจ (Business Continuity Management: BCM) และเกณฑ์มาตรฐานสากลที่สถาบันยึดถือปฏิบัติ

๒) ขอบเขตปัจจัยสมมติฐาน สมมติฐานครอบคลุมถึงปัจจัยสำคัญทุกมิติที่เกี่ยวข้อง ได้แก่ สถานที่ปฏิบัติงานหลักและสถานที่สำรอง ความต้องการและขีดความสามารถของทรัพยากร ความพึ่งพาอาศัยกันระหว่างระบบงานและผู้ให้บริการภายนอก (Dependencies) ความคุ้มค่าและกรอบงบประมาณ ตลอดจนกลยุทธ์ในการตอบสนอง เผชิญเหตุ และการกู้คืนระบบงานวิกฤต

๓) การสื่อสาร ข้อตกลง และการทดสอบซักซ้อม สมมติฐานทั้งหมดจะต้องได้รับการสื่อสาร ทำความเข้าใจ และลงนามตกลงร่วมกันโดยผู้มีส่วนได้ส่วนเสียทุกภาคส่วน ทั้งนี้ ในส่วนของสมมติฐานที่เกี่ยวข้องกับกลยุทธ์การตอบสนองและการกู้คืนระบบ จะต้องได้รับการทดสอบและประเมินผลจริงอย่างสม่ำเสมอ โดยถือเป็นส่วนหนึ่งของกำหนดการฝึกซ้อมแผนบริหารความต่อเนื่องทางธุรกิจ (BCP Exercise Schedule) ประจำปีของสถาบัน

๑.๕ ความเป็นเจ้าของ

สถาบันระหว่างประเทศเพื่อการค้าและการพัฒนา (องค์การมหาชน) เป็นเจ้าของและผู้ถือสิทธิการบริการ ผู้รับผิดชอบดำเนินการโดยบริษัทและหรือผู้ที่ได้รับแต่งตั้งจากสถาบัน

๑.๖ ความพร้อมใช้งานของแผน

เพื่อให้แผนบริหารความต่อเนื่องทางธุรกิจด้านเทคโนโลยีสารสนเทศ (BCP ด้าน IT) ฉบับทบทวน พ.ศ. ๒๕๖๙ มีความพร้อมใช้งาน และสามารถนำไปปฏิบัติได้อย่างทันท่วงทีเมื่อเกิดภาวะฉุกเฉินหรือภาวะวิกฤต สถาบันได้กำหนดบุคคลผู้ถือครองเอกสาร และมาตรการจัดเก็บรักษาเอกสารไว้ ประกอบด้วย

๑) บุคคลผู้ถือครองและเข้าถึงเอกสารแผน

เอกสารแผน BCP ฉบับสมบูรณ์จะได้รับการจัดสรรและแจกจ่ายให้แก่บุคคลและกลุ่มงานที่เกี่ยวข้อง เพื่อใช้ในการปฏิบัติงานและตัดสินใจ ดังนี้

- คณะผู้บริหารระดับสูง เพื่อรับทราบแนวทาง สิทธิอำนาจในการสั่งการ และใช้ประกอบการตัดสินใจในภาวะวิกฤต
- หัวหน้าฝ่าย / หัวหน้ากลุ่มงาน ที่รับผิดชอบโดยตรงต่อกระบวนงานวิกฤตที่ระบุไว้ในแผน BCP
- คณะทำงานบริหารความต่อเนื่องทางธุรกิจ (BCP Team / IT Recovery Team) ซึ่งเป็นผู้รับผิดชอบหลักในการขับเคลื่อน ดำเนินการ และกู้คืนระบบตามแผน
- เจ้าหน้าที่เทคโนโลยีสารสนเทศ ผู้ดูแลระบบสารสนเทศ ฐานข้อมูลวิกฤต และโครงสร้างพื้นฐานดิจิทัล
- เจ้าหน้าที่รักษาความปลอดภัย ผู้ดูแลความปลอดภัยทางกายภาพ อาคารสถานที่ และความปลอดภัยของบุคลากร

๒)วิธีการจัดเก็บและการเข้าถึงเอกสารแผน (Storage and Access Protocols)

การจัดเก็บและการเข้าถึงเอกสารแผน BCP ให้ดำเนินการผ่าน ๒ ช่องทางหลัก ได้แก่

- สำเนาอิเล็กทรอนิกส์ (Soft Copy) นักเทคโนโลยีสารสนเทศ หรือผู้ได้รับมอบหมายจากสถาบัน มีหน้าที่จัดเก็บไฟล์เอกสารไว้ในระบบ Google Drive / Cloud Storage ของสถาบันที่มีมาตรการความปลอดภัยสูง โดยกำหนดตั้งค่าให้สามารถเข้าถึงได้จากภายนอกสถาบันได้อย่างปลอดภัยผ่านการยืนยันตัวตน มีการสำรองข้อมูลเป็นประจำ และสำรองไว้ในระบบที่ปลอดภัย ตลอดจนจำกัดสิทธิ์การเข้าถึง เพื่อให้เฉพาะผู้ที่เกี่ยวข้องและได้รับอนุญาตเท่านั้นที่สามารถเปิดอ่านได้
- สำเนาเอกสารฉบับพิมพ์ (Hard Copy) นักเทคโนโลยีสารสนเทศ หรือผู้ได้รับมอบหมายจากสถาบัน มีหน้าที่จัดเก็บสำเนาเอกสารฉบับพิมพ์ไว้ในตู้เก็บเอกสารที่มีความมั่นคงปลอดภัยและเข้าถึงได้ง่ายในภาวะฉุกเฉิน และต้องจัดทำบัญชีรายชื่อผู้ได้รับสำเนาเอกสาร (Controlled Distribution List) เพื่อให้สามารถควบคุมและอัปเดตเอกสารให้เป็นปัจจุบันได้อย่างเป็นระบบผู้มีรายละเอียดของแผนบริหารความต่อเนื่องทางธุรกิจ

๑.๗ เอกสารที่เกี่ยวข้อง

๑) นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ พ.ศ. ๒๕๖๙
๒) แผนรับมือเหตุภัยคุกคามทางไซเบอร์ พ.ศ. ๒๕๖๗
๓) กรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Framework) พ.ศ. ๒๕๖๗

๒. ภูมิหลังของสถาบัน

๒.๑ คำอธิบายบริการทางอิเล็กทรอนิกส์ของสถาบัน

การให้บริการต่าง ๆ ของสถาบันผ่านช่องทางอิเล็กทรอนิกส์ เช่น อินเทอร์เน็ต แอปพลิเคชันบนมือถือ หรือระบบออนไลน์ต่าง ๆ เพื่ออำนวยความสะดวก รวดเร็ว และเข้าถึงง่ายยิ่งขึ้นสำหรับผู้ใช้บริการ ประกอบด้วย

๑) เว็บไซต์ หมายถึง ช่องทางหลักเพื่อนำเสนอข้อมูล ข่าวสาร กิจกรรม และบริการที่เกี่ยวข้องกับบทบาท หน้าที่ และเป้าหมายเกี่ยวกับสถาบัน เช่น www.itd.or.th, www.bcgconnex.com เป็นต้น

๒) แอปพลิเคชันบนมือถือ หมายถึง โปรแกรมหรือซอฟต์แวร์เพื่ออำนวยความสะดวกในการให้บริการ หรือติดต่อสื่อสารกับกลุ่มเป้าหมายของสถาบันผ่านอุปกรณ์ต่าง ๆ เช่น สมาร์ทโฟน แท็บเล็ต ตัวอย่างแอปพลิเคชันของสถาบัน Prompt Pass App

๓) ฐานข้อมูลออนไลน์ หมายถึง ฐานข้อมูลให้ผู้ใช้เข้าถึงฐานข้อมูลเฉพาะของสถาบัน

๔) อีเมล ใช้ในการติดต่อสื่อสารระหว่างสถาบันกับผู้ใช้บริการ

๕) ฟอรัมออนไลน์ เป็นพื้นที่สำหรับผู้ใช้บริการแลกเปลี่ยนความคิดเห็นและสอบถามข้อมูล

๖) ระบบผู้เชี่ยวชาญออนไลน์ ใช้สำหรับการประชุม สัมมนา หรือการเรียนการสอนทางไกล

๗) การฝึกอบรมออนไลน์ ให้บริการหลักสูตรฝึกอบรมและพัฒนาทักษะต่าง ๆ ผ่านช่องทางออนไลน์

๒.๒ จุดมุ่งหมายของสถาบัน

๑) จัดการศึกษาอบรมและให้การสนับสนุนเพื่อการค้นคว้าวิจัยแก่บุคลากรของประเทศต่างๆ โดยเฉพาะในภูมิภาค เอเชีย ด้านการค้าระหว่างประเทศ การเงิน การคลัง การลงทุน การพัฒนา และสาขาอื่นที่เกี่ยวข้อง เพื่อให้บุคลากรเหล่านั้นสามารถปฏิบัติงานในหน้าที่ได้อย่างมีประสิทธิภาพ สอดคล้องกับกระแสโลกาภิวัตน์และแนวทางการยกเลิกข้อจำกัดทางการค้าต่าง ๆ

๒) ให้ความช่วยเหลือแก่ประเทศกำลังพัฒนาโดยเฉพาะในภูมิภาคเอเชีย เพื่อสร้างเสริมศักยภาพและความสามารถ ในการกำหนดนโยบายด้านเศรษฐกิจที่เหมาะสมร่วมกัน และการกำหนดมาตรการทางกฎหมายที่สอดคล้องกับนโยบายดังกล่าวได้

๓) ส่งเสริมและสนับสนุนความร่วมมือทางเศรษฐกิจในระดับภูมิภาค และสร้างความเป็นเอกภาพโดยการแลกเปลี่ยนประสบการณ์และความรู้

๔) เป็นศูนย์กลางจัดการฝึกอบรม และกิจกรรมเสริมศักยภาพต่าง ๆ ร่วมกับ สำนักงานเลขาธิการสหประชาชาติ ว่าด้วยการค้าและการพัฒนา และองค์การอื่นที่เกี่ยวข้องสถาบันมุ่งเน้นการให้บริการที่สร้างคุณค่าและประโยชน์ให้กับผู้รับบริการ

๒.๓ วัตถุประสงค์หลักของสถาบัน

๑) จัดการศึกษาอบรมและให้การสนับสนุนเพื่อการค้นคว้าวิจัยแก่บุคลากรของประเทศต่าง ๆ โดยเฉพาะในภูมิภาคเอเชีย ด้านการค้าระหว่างประเทศ การเงิน การคลัง การลงทุน การพัฒนา และสาขาอื่นที่เกี่ยวข้อง เพื่อให้บุคลากรเหล่านั้นสามารถปฏิบัติงานในหน้าที่ได้อย่างมีประสิทธิภาพ สอดคล้องกับกระแสโลกาภิวัตน์และแนวทางการลดข้อจำกัดทางการค้าต่าง ๆ

๒) ให้ความช่วยเหลือแก่ประเทศกำลังพัฒนาโดยเฉพาะในภูมิภาคเอเชีย เพื่อสร้างเสริมทักษะและความสามารถในการกำหนดนโยบายด้านเศรษฐกิจที่เหมาะสมร่วมกัน และการกำหนดมาตรการทางกฎหมายที่สอดคล้องกับนโยบายดังกล่าวได้

๓) ส่งเสริมและสนับสนุนความร่วมมือทางเศรษฐกิจในระดับภูมิภาค และสร้างความเป็นเอกภาพโดยการแลกเปลี่ยนประสบการณ์และความรู้

๔) เป็นศูนย์กลางจัดการฝึกอบรม และกิจกรรมเสริมศักยภาพต่าง ๆ ร่วมกับสำนักงานเลขาธิการสหประชาชาติว่าด้วยการค้าและการพัฒนา และองค์การอื่นที่เกี่ยวข้อง

๒.๔ โครงสร้างองค์กร

สถาบันเป็นองค์กรที่ไม่แสวงหากำไร จัดตั้งขึ้นภายใต้กฎหมายของรัฐบาลไทยโดยมีสถานะเป็นองค์การมหาชน สถาบันดำเนินงานโดยอาศัยความร่วมมืออย่างใกล้ชิดกับรัฐบาลไทย อังค์ถัด องค์กรระหว่างประเทศอื่น ๆ และองค์กรระดับภูมิภาค และมีโครงสร้างการบริหารดังนี้

๑) คณะกรรมการ (Board of Directors) เป็นส่วนสูงสุดในการกำหนดนโยบายและทิศทางของสถาบัน หน้าที่หลักคือการกำกับดูแลการดำเนินงาน การกำหนดวิสัยทัศน์ พันธกิจ และเป้าหมายระยะยาว รวมถึงการอนุมัติงบประมาณและแผนยุทธศาสตร์

๒) คณะผู้บริหาร (Executive Management) เป็นผู้รับผิดชอบในการนำนโยบายที่คณะกรรมการกำหนดไปปฏิบัติจริง รวมถึงการบริหารจัดการทรัพยากรบุคคล การเงิน และการดำเนินงานประจำวัน เพื่อให้บรรลุเป้าหมายที่วางไว้

๓) สำนัก (Office) เป็นการแบ่งแยกการทำงานออกเป็นส่วนย่อย ๆ ตามหน้าที่รับผิดชอบ เพื่อให้การบริหารจัดการมีประสิทธิภาพและเฉพาะทางมากขึ้น แต่ละสำนักจะมีบทบาทและหน้าที่ที่ชัดเจน

๔) บุคลากร (Staff) คือเจ้าหน้าที่ทั้งหมดของสถาบันที่ปฏิบัติหน้าที่ในส่วนงานต่าง ๆ เพื่อขับเคลื่อนภารกิจของสถาบัน ตั้งแต่ผู้บริหาร เจ้าหน้าที่ พนักงาน ไปจนถึงเจ้าหน้าที่สนับสนุน

๓. การกำกับดูแลและนโยบายการบริหารความต่อเนื่องทางธุรกิจ (Business Continuity Management: BCM)

๓.๑ คำแถลงนโยบาย

สถาบันตระหนักถึงความสำคัญของการกำกับดูแลกิจการที่ดี และการบริหารความต่อเนื่องทางธุรกิจ เพื่อสร้างความเชื่อมั่นแก่ผู้มีส่วนได้ส่วนเสียทุกกลุ่ม และเพื่อความยั่งยืนขององค์กร จึงได้กำหนดนโยบายฉบับนี้ขึ้น เพื่อเป็นแนวทางในการปฏิบัติงานของคณะกรรมการ ผู้บริหาร และผู้ปฏิบัติหน้าที่ของสถาบัน

๓.๒ บทบาทและความรับผิดชอบ (Roles and Responsibilities)

๓.๒.๑ ผู้อำนวยการกำกับดูแลและนโยบายการบริหารความต่อเนื่องทางธุรกิจของสถาบัน

๑) กำหนดและอนุมัตินโยบายการกำกับดูแลและ BCM
๒) กำกับดูแลการดำเนินงานตามนโยบายให้เป็นไปอย่างมีประสิทธิภาพ
๓) ประเมินความเสี่ยงและผลกระทบที่อาจเกิดขึ้นกับธุรกิจ
๔) อนุมัติแผน BCM และจัดสรรทรัพยากรที่จำเป็น
๕) ติดตามและประเมินผลการดำเนินงานของแผน BCM
๖) ผู้นำในการสร้างวัฒนธรรมองค์กรที่ให้ความสำคัญกับการกำกับดูแลและ BCM
๗) ผู้ให้การสนับสนุนและทรัพยากรที่จำเป็นสำหรับการดำเนินแผน BCM

๓.๒.๒ ผู้บริหารระดับสูง

๑) นำนโยบายการกำกับดูแลและ BCM ไปปฏิบัติให้เกิดผล
๒) จัดทำแผน BCM และดำเนินการตามแผน
๓) มอบหมายงานและกำกับดูแลการทำงานของทีม BCM
๔) รายงานผลการดำเนินงานของแผน BCM ต่อคณะกรรมการ
๕) ควบคุมดูแลให้มีการทบทวนและปรับปรุงแผนอย่างสม่ำเสมอ
๖) ผู้บริหารจัดการแผน BCM และประสานงานกับสถาบันต่าง ๆ

๗) ผู้ตัดสินใจในสถานการณ์ฉุกเฉิน

๓.๒.๓ ทีมบริหารความต่อเนื่องทางธุรกิจ (BCM Team)

๑) ประเมินความเสี่ยงและผลกระทบ
๒) จัดทำและปรับปรุงแผน BCM
๓) ทดสอบและฝึกอบรมแผน BCM
๔) ประสานงานกับสถาบันต่าง ๆ ในการดำเนินแผน BCM
๕) รวบรวมข้อมูลและจัดทำรายงานผลการดำเนินงาน
๖) ผู้ปฏิบัติงานตามแผน BCM และผู้ให้ข้อมูลสนับสนุน

๓.๒.๔ ผู้ปฏิบัติหน้าที่ของสถาบัน

๑) ปฏิบัติตามนโยบายและแผน BCM
๒) รายงานเหตุการณ์ที่อาจส่งผลกระทบต่อธุรกิจ
๓) เข้าร่วมการฝึกอบรมและทดสอบแผน BCM
๔) ให้ความร่วมมือในการดำเนินการตามแผนที่วางไว้

๓.๓ การกำกับดูแล

เพื่อให้มั่นใจว่าสถาบันมีความพร้อมในการรับมือกับเหตุการณ์ที่ไม่คาดคิด และสามารถดำเนินธุรกิจได้อย่างราบรื่นควรการกำกับดูแลอย่างน้อย ดังนี้

๓.๓.๑ การติดตามการปฏิบัติตามนโยบาย

๑) ทำการตรวจสอบและประเมินผลการปฏิบัติตามนโยบายอย่างสม่ำเสมอ

๓.๓.๒ การติดตามการปฏิบัติตามข้อกำหนด

๑) ตรวจสอบการปฏิบัติตามข้อกำหนดทางกฎหมาย ระเบียบข้อบังคับ และมาตรฐานที่เกี่ยวข้องกับ BCM

๒) ทำการประเมินผลการปฏิบัติตามข้อกำหนดและระบุช่องว่างที่ต้องปรับปรุง

๓.๓.๓ การรายงานผลการปฏิบัติงาน

๑) จัดทำรายงานผลการปฏิบัติงานการบริหารความต่อเนื่องทางธุรกิจ (Business Continuity Management) เพื่อนำเสนอต่อผู้บริหาร

๒) รายงานควรครอบคลุมถึงผลการประเมินความเสี่ยง ผลการทดสอบแผนการบริหารความต่อเนื่องทางธุรกิจ และผลการปฏิบัติตามนโยบายและข้อกำหนด

๓.๓.๔ การปรับปรุงอย่างต่อเนื่อง

๑) นำผลการติดตามและรายงานมาใช้ในการปรับปรุงแผนการบริหารความต่อเนื่องทางธุรกิจและกระบวนการกำกับดูแล

๒) ทำการทบทวนและปรับปรุงนโยบายการบริหารความต่อเนื่องทางธุรกิจให้ทันสมัยอยู่เสมอ

๔. ทบทวนแผนและบำรุงรักษา

แผนการบริหารความต่อเนื่องทางธุรกิจ (Business Continuity Management: BCM) นี้จะได้รับการทบทวนเป็นประจำทุกปีเพื่อให้แน่ใจว่าข้อมูลลำดับการสื่อสาร (Call Trees) ตำแหน่ง และโครงสร้างยังคงถูกต้อง การวิเคราะห์ผลกระทบทางธุรกิจ (Business Impact Analyses: BIA) ควรได้รับการทบทวนทุกปีเพื่อให้แน่ใจว่าหน้าที่ทางธุรกิจที่สำคัญสะท้อนถึงจุดมุ่งหมายและวัตถุประสงค์ของสถาบัน

๕. การฝึกอบรมและการฝึกซ้อมแผน

๕.๑ การฝึกอบรม

๑) มีการจัดทำการบรรยายสรุปเพื่อสร้างความตระหนักรู้เกี่ยวกับการบริหารความต่อเนื่องทางธุรกิจให้กับบุคลากรในองค์กร (Business Continuity Management Awareness Briefing) สำหรับบุคลากรทุกคน ปีละครั้ง สำหรับผู้เข้าร่วมใหม่ การบรรยายสรุปนี้จะดำเนินการเป็นส่วนหนึ่งของแผนงานการปฐมนิเทศ

๒) การฝึกอบรมสำหรับผู้ที่อยู่ในทีมความต่อเนื่องทางธุรกิจจะรวมอยู่ในแผนงานการฝึกซ้อมแผน

๓) การบรรยายสรุปจะดำเนินการก่อนการฝึกซ้อมแผนเพื่อให้ข้อมูลพื้นฐานและบริบท รวมทั้งการเข้าร่วมฝึกซ้อมยังช่วยยกระดับทักษะการปฏิบัติงานของบุคลากรไปในตัว

๕.๒ การฝึกซ้อมแผน

๑) การฝึกซ้อมแผนช่วยตรวจสอบประสิทธิภาพของการจัดการความต่อเนื่องทางธุรกิจทุกด้านทุกจุดประสงค์ของแผน

๒) ตรวจสอบให้แน่ใจว่าแผนเป็นปัจจุบัน ได้รับการพิสูจน์และดูแลโดยบุคคลที่ต้องการใช้เมื่อเกิดเหตุภัยคุกคามทางไซเบอร์

๓) เปิดโอกาสให้บุคลากร ซักซ้อมแผนเพื่อสร้างความคุ้นเคยกับปฏิบัติการเผชิญเหตุ พัฒนาการทำงานเป็นทีมอย่างมีประสิทธิภาพ และสร้างความมั่นใจ

๔) ประเมินและตรวจสอบ ความสามารถด้านความต่อเนื่องทางธุรกิจในการตอบสนองต่อเหตุภัยคุกคามทางไซเบอร์ที่เกิดขึ้นจริง

๕) ระบุข้อบกพร่องใน กลยุทธ์และแผนความต่อเนื่องทางธุรกิจเพื่อให้สามารถดำเนินการแก้ไขได้

๖) การฝึกซ้อมแผนเป็นประจำทุกปี

๖. ลำดับความสำคัญและกลยุทธ์ความต่อเนื่องทางธุรกิจ

การระบุและจัดลำดับความสำคัญของกระบวนการทางธุรกิจ ทรัพยากร และกิจกรรมต่าง ๆ ที่มีความสำคัญต่อการดำเนินงานของสถาบัน หากเกิดเหตุการณ์การหยุดชะงัก (Disruption) จะต้องให้ความสำคัญกับการฟื้นฟูสิ่งเหล่านี้ก่อนเป็นอันดับแรก โดยทั่วไปแล้ว การจัดลำดับความสำคัญจะพิจารณาจากปัจจัยดังนี้

๑) การเริ่มต้น (Initiation) กำหนดขอบเขต เป้าหมาย และทรัพยากร

๒) การวิเคราะห์ผลกระทบทางธุรกิจ (BIA) ระบุและประเมินผลกระทบต่อธุรกิจ

๓) การประเมินความเสี่ยง (Risk Assessment) ระบุและประเมินความเสี่ยงที่เกี่ยวข้อง

๔) การพัฒนากลยุทธ์ (Strategy Development) เลือกกลยุทธ์ที่เหมาะสม

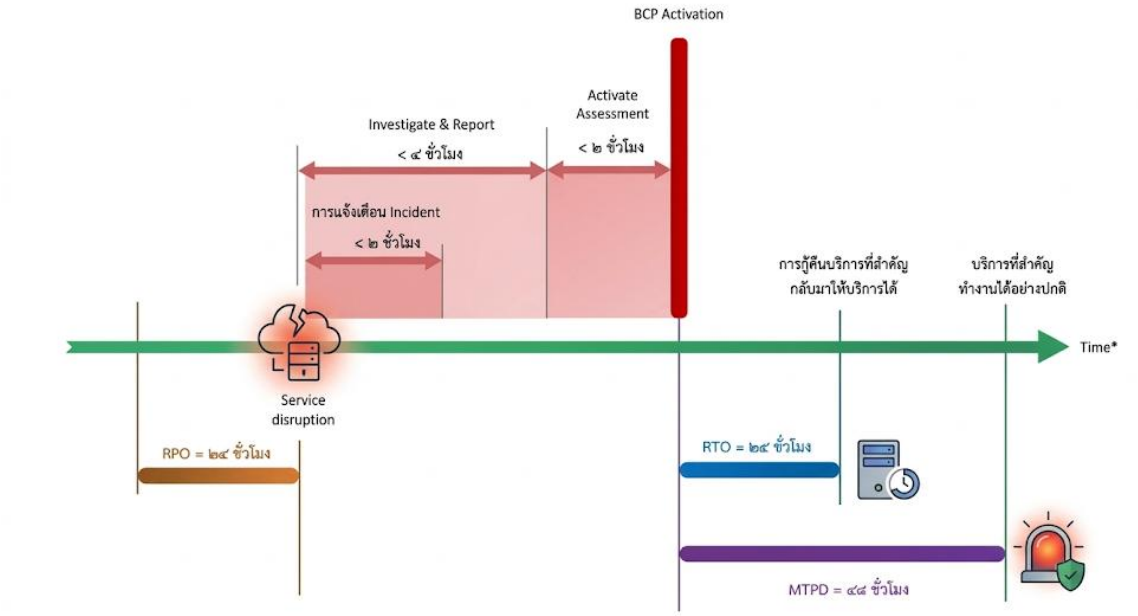
๕) การพัฒนาแผน (Plan Development) จัดทำแผน BCM ที่ครอบคลุม

๖) การทดสอบและการฝึกอบรม (Testing and Training) ทดสอบแผนและฝึกอบรมบุคลากร

๗) การบำรุงรักษาและการปรับปรุง (Maintenance and Improvement)

๖.๑ หน้าที่ทางธุรกิจที่สำคัญ

การวิเคราะห์ผลกระทบทางธุรกิจ (Business Impact Analysis: BIA) ดำเนินการเพื่อประเมินผลกระทบที่อาจเกิดขึ้น ของการหยุดชะงักของบริการ และเพื่อจัดลำดับความสำคัญของกิจกรรมทางธุรกิจและบริการสำหรับการกู้คืน รายละเอียดการวิเคราะห์ BIA ตามข้อ ๙ หน้า ๖๑ และรายงานการวิเคราะห์ผลกระทบทางธุรกิจ (Business Continuity Strategies) ดังแสดง หน้า ๕๒ โดยสถาบันได้กำหนดความสัมพันธ์ระหว่างเหตุบริการทางธุรกิจที่สำคัญ ในรูปที่ ๒



รูปที่ ๒ ภาพความสัมพันธ์ระหว่างเหตุ (Incident) และระยะเวลาเป้าหมายในการกู้คืนบริการที่สำคัญ

ตารางที่ ๑ ตารางหน้าที่ทางธุรกิจที่สำคัญ (Critical Business Functions)

บริการทางธุรกิจที่สำคัญ (Critical Business Service)	คำอธิบาย	ความสำคัญ	ผลกระทบจากการสูญเสีย Impact of loss (ความสูญเสียในแง่ของการเงิน บุคลากร การสูญเสียชื่อเสียง ฯลฯ)	RPO (๑)	RTO (๒)	MTPD (๓)
ระบบเว็บไซต์สถาบัน	ศูนย์กลางข้อมูลข่าวสารและการพัฒนาศักยภาพด้านการค้า โดยให้บริการคลังงานวิจัยและรายงานวิเคราะห์เชิงลึก หลักสูตรอบรม/สัมมนาเพื่อยกระดับทักษะบุคลากรทั้งภาครัฐและเอกชน และกิจกรรมความร่วมมือระหว่างประเทศต่างๆ	ต่ำ	• สูญเสียความน่าเชื่อถือ • ผู้รับบริการจะจัดหาแหล่งบริการใหม่ • การสูญเสียงานที่อาจเกิดขึ้น (หลังจาก ๒ สัปดาห์)	๒๔ ชั่วโมง	๒๔ ชั่วโมง	๔๘ ชั่วโมง
ระบบเว็บไซต์ BCG CONNEX	แพลตฟอร์มดิจิทัล ที่เป็นศูนย์กลางเชื่อมโยง และสร้างเครือข่ายความร่วมมือทางธุรกิจสำหรับผู้ประกอบการ MSMEs และผู้ประกอบการรายย่อยในกลุ่มอุตสาหกรรมแปรรูปอาหารและอาหารแห่งอนาคต ตามแนวคิดโมเดลเศรษฐกิจ BCG รวมถึงการเป็นแหล่งข้อมูลองค์ความรู้เพื่อยกระดับขีดความสามารถการแข่งขันอย่างยั่งยืน	ต่ำ	• สูญเสียความน่าเชื่อถือ • ผู้รับบริการจะจัดหาแหล่งบริการใหม่ • การสูญเสียงานที่อาจเกิดขึ้น (หลังจาก ๒ สัปดาห์)	๒๔ ชั่วโมง	๒๔ ชั่วโมง	๔๘ ชั่วโมง

บริการทางธุรกิจที่สำคัญ (Critical Business Service)	คำอธิบาย	ความสำคัญ	ผลกระทบจากการสูญเสีย Impact of loss (ความสูญเสียในแง่ของการเงิน บุคลากร การสูญเสียชื่อเสียง ฯลฯ)	RPO (๑)	RTO (๒)	MTPD (๓)
ระบบบริหารจัดการบุคลากร (Humansoft)	การบริหารจัดการเจ้าหน้าที่ และระบบลงเวลา และระบบที่เกี่ยวข้องกับงานบุคคล	กลาง	• สูญเสียความน่าเชื่อถือ • การขัดข้องการจัดการจากบุคลากร • ผู้รับบริการจะจัดหาแหล่งบริการใหม่ • การสูญเสียงานที่อาจเกิดขึ้น (หลังจาก ๒ สัปดาห์)	๒๔ ชั่วโมง	๑๒ ชั่วโมง	๗๒ ชั่วโมง
ระบบจัดการงบประมาณ (e-Budget)	ระบบสารสนเทศที่ช่วยรวมศูนย์ฐานข้อมูลด้านงบประมาณ การเงิน บัญชี และพัสดุเข้าด้วยกัน แบบเป็นปัจจุบัน (Real-time) ลดความซ้ำซ้อนและเพิ่มความรวดเร็วในกระบวนการทำงาน ยกระดับความโปร่งใสผ่านระบบอนุมัติอิเล็กทรอนิกส์ พร้อมสรุปผลการใช้จ่ายงบประมาณที่แม่นยำ เพื่อสนับสนุนการตัดสินใจของผู้บริหาร บนระบบ Cloud Server	กลาง	• สูญเสียความน่าเชื่อถือ • การดำเนินการงบประมาณติดขัด • ผู้รับบริการจะจัดหาแหล่งบริการใหม่ • การสูญเสียงานที่อาจเกิดขึ้น (หลังจาก ๒ สัปดาห์)	๒๔ ชั่วโมง	๑๒ ชั่วโมง	๗๒ ชั่วโมง

บริการทางธุรกิจที่สำคัญ (Critical Business Service)	คำอธิบาย	ความสำคัญ	ผลกระทบจากการสูญเสีย Impact of loss (ความสูญเสียในแง่ของการเงิน บุคลากร การสูญเสียชื่อเสียง ฯลฯ)	RPO (๑)	RTO (๒)	MTPD (๓)
ระบบ Prompt Pass	การสืบค้นผู้เชี่ยวชาญ และดำเนินการให้คำปรึกษา เข้าร่วมงานหรือกิจกรรมของสถาบัน เว็บไซต์และแอปพลิเคชันคลินิกเสมือนจริงให้คำปรึกษาผู้ประกอบการ SMEs เพื่อการส่งออก (SME virtual clinic) ด้วยการรวบรวมนักวิชาการ/ผู้เชี่ยวชาญทั้งในประเทศและภูมิภาค มาให้คำปรึกษาผู้ประกอบการในรูปแบบออนไลน์ผ่านข้อความเสียงสนทนาหรือภาพและเสียง มุ่งสนับสนุนผู้ประกอบการ และ SME แบบครบวงจร ผ่าน ๓ บริการหลัก ได้แก่ การนัดหมายปรึกษาผู้เชี่ยวชาญแบบออนไลน์, ระบบลงทะเบียนเข้าร่วมกิจกรรม และ ศูนย์รวมคลังความรู้เชิงลึกเพื่อการพัฒนาธุรกิจ	กลาง	• สูญเสียความน่าเชื่อถือ • ผู้รับบริการจะจัดหาแหล่งบริการใหม่ • การสูญเสียงานที่อาจเกิดขึ้น (หลังจาก ๒ สัปดาห์)	๒๔ ชั่วโมง	๑๒ ชั่วโมง	๗๒ ชั่วโมง
ระบบจัดการสำนักงาน (e-Office)	ระบบสำนักงานอเล็กทรอนิกส์ที่ช่วยทำให้การดำเนินงานของสำนักงานเป็นไปอย่างมีประสิทธิภาพ ราบรื่น และเป็นระบบระเบียบมากขึ้น เช่น ระบบสารบรรณ ระบบจองรถ ระบบจองห้องประชุม	กลาง	• สูญเสียความน่าเชื่อถือ • ผู้รับบริการจะแจ้งเหตุไปยัง สพร. • การสูญเสียงานที่อาจเกิดขึ้น (หลังจาก ๒ สัปดาห์)	๒๔ ชั่วโมง	๑๒ ชั่วโมง	๗๒ ชั่วโมง

หมายเหตุ: **๑) จุดหมายของการกู้คืนข้อมูล (RPO: Recovery Point Objective)** คือ จุดย้อนเวลากลับไปล่าสุด ที่ข้อมูลควรจะได้รับการกู้คืนกลับมาได้ภายหลังเกิดเหตุการณ์ภัยพิบัติหรือความล้มเหลวของระบบ RPO จะเป็นตัวกำหนดว่าสถาบันสามารถยอมรับการสูญเสียข้อมูลได้มากน้อยเพียงใด โดยวัดเป็นช่วงเวลา

๒) จุดหมายของระยะเวลาการกู้คืน (RTO: Recovery Time Objective) คือ ระยะเวลาสูงสุดที่ยอมรับได้ สำหรับการกู้คืนระบบ แอปพลิเคชัน และการเข้าถึงข้อมูลให้กลับมาใช้งานได้ตามปกติภายหลังเกิดเหตุการณ์ RTO จะเป็นตัวกำหนดว่าสถาบันสามารถยอมรับการหยุดชะงักของธุรกิจได้นานเท่าใด โดยวัดเป็นช่วงเวลา

๓) ระยะเวลาหยุดทำงานสูงสุดที่ยอมรับได้ (MTPD: Maximum Tolerable Period of Disruption หรือ MRPD: Maximum Permissible Downtime) คือ ระยะเวลาที่นานที่สุด ที่องค์กรสามารถยอมรับได้ว่าระบบหรือกระบวนการทางธุรกิจที่สำคัญจะหยุดทำงาน ก่อนที่จะส่งผลกระทบต่อธุรกิจอย่างรุนแรงจนไม่สามารถฟื้นตัวได้ MRPD จะพิจารณาถึงผลกระทบทางธุรกิจที่อาจเกิดขึ้นจากการหยุดทำงาน

ตารางที่ ๒ ตารางบริการสำคัญและประเภทของการพึ่งพา (Type of Dependency)

ลำดับที่	บริการทางธุรกิจที่สำคัญ (Critical Business Service)	ชื่อผู้รับผิดชอบ	ชื่อผู้ให้บริการภายนอก	ประเภทของการพึ่งพา	
				ภายใน หรือ ภายนอก	บริการสำคัญเป็นส่วนต้นน้ำหรือปลายน้ำของฟังก์ชันการทำงานที่สำคัญของบริษัท (Critical Service is upstream/downstream to the Business function)
๑	ระบบเว็บไซต์สถาบัน	สถาบัน	สำนักงานคณะกรรมการดิจิทัลเพื่อเศรษฐกิจและสังคมแห่งชาติ	Cloud Service	การส่งถ่ายข้อมูลระบบ
๒	ระบบเว็บไซต์ BCG CONNEX	สถาบัน	บริษัท ซีเอส ล็อกซอินโฟ จำกัด (มหาชน) (CS Loxinfo Public Company Limited)	Cloud Service	การส่งถ่ายข้อมูลระบบ
๓	ระบบบริหารจัดการบุคลากร (Humansoft)	สถาบัน	บริษัท ฮิวแมนซอฟท์ จำกัด	Cloud Service	การส่งถ่ายข้อมูลระบบ
๔	ระบบสารสนเทศในการบริหารจัดการองค์กร ด้านงบประมาณ การเงิน บัญชี และพัสดุ (e-Budget)	สถาบัน	บริษัท คลาวด์ เอชเอ็ม จำกัด	Cloud Service	การส่งถ่ายข้อมูลระบบ
๕	ระบบ Prompt Pass	สถาบัน	บริษัท คลาวด์ เอชเอ็ม จำกัด	Cloud Service	การส่งถ่ายข้อมูลระบบ
๖	ระบบเว็บไซต์ Prompt Pass	สถาบัน	บริษัท คลาวด์ เอชเอ็ม จำกัด	Cloud Service	การส่งถ่ายข้อมูลระบบ
๗	ระบบจัดการสำนักงาน	สถาบัน	สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน) หรือ สพร.	Cloud Service	การส่งถ่ายข้อมูลระบบ

๗. การเปิดใช้งานแผน

๗.๑ เกณฑ์การเปิดใช้งาน

แผนนี้เปิดใช้งานเมื่อเกิดการหยุดชะงัก และเมื่อฟังก์ชันทางธุรกิจที่สำคัญ (Critical Business Function: CBF) ที่ระบุล่วงหน้ามีหรือคาดการณ์ว่าจะเกินระยะเวลาสูงสุดที่ยอมให้ธุรกิจหยุดชะงัก (Maximum Tolerable Downtime: MTD)

๗.๒ สิทธิ์ในการเปิดใช้งาน

อำนาจในการเปิดใช้งานแผนนี้ขึ้นอยู่กับ ผู้บริหารเทคโนโลยีสารสนเทศระดับกรม หรือสูงกว่า

๗.๓ การยกระดับ (Escalation)

เมื่อดำเนินการตามกลยุทธ์ความต่อเนื่องทางธุรกิจที่คาดว่าจะส่งผลกระทบต่อบริการ อาจต้องมีการประสานงานระดับกรม ในกรณีเหล่านี้ ให้แจ้งสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ

๗.๔ การระดมทีมความต่อเนื่องทางธุรกิจ (Business Continuity Team: BCT)

ในการเปิดใช้งานแผนนี้ ทีมความต่อเนื่องทางธุรกิจ (BCT) จะระดมพล ณ ห้องประชุมบอร์ด อาคารวิทยพัฒนา สถาบันระหว่างประเทศเพื่อการค้าและการพัฒนา (องค์การมหาชน)

๗.๕ จุดควบคุมเหตุภัยคุกคามทางไซเบอร์

จุดควบคุมเหตุภัยคุกคามทางไซเบอร์ (Incident Control Point: ICP) ตำแหน่งที่กำหนดไว้ล่วงหน้าซึ่งทีมเผชิญเหตุจะประสานงานกิจกรรมในสถานที่เมื่อเปิดใช้งาน BCP

จุดควบคุมเหตุภัยคุกคามทางไซเบอร์จะจัดตั้งขึ้นที่หนึ่งในสองแห่ง หากเป็นไปได้ ทั้งนี้ขึ้นอยู่กับลักษณะของเหตุภัยคุกคามทางไซเบอร์

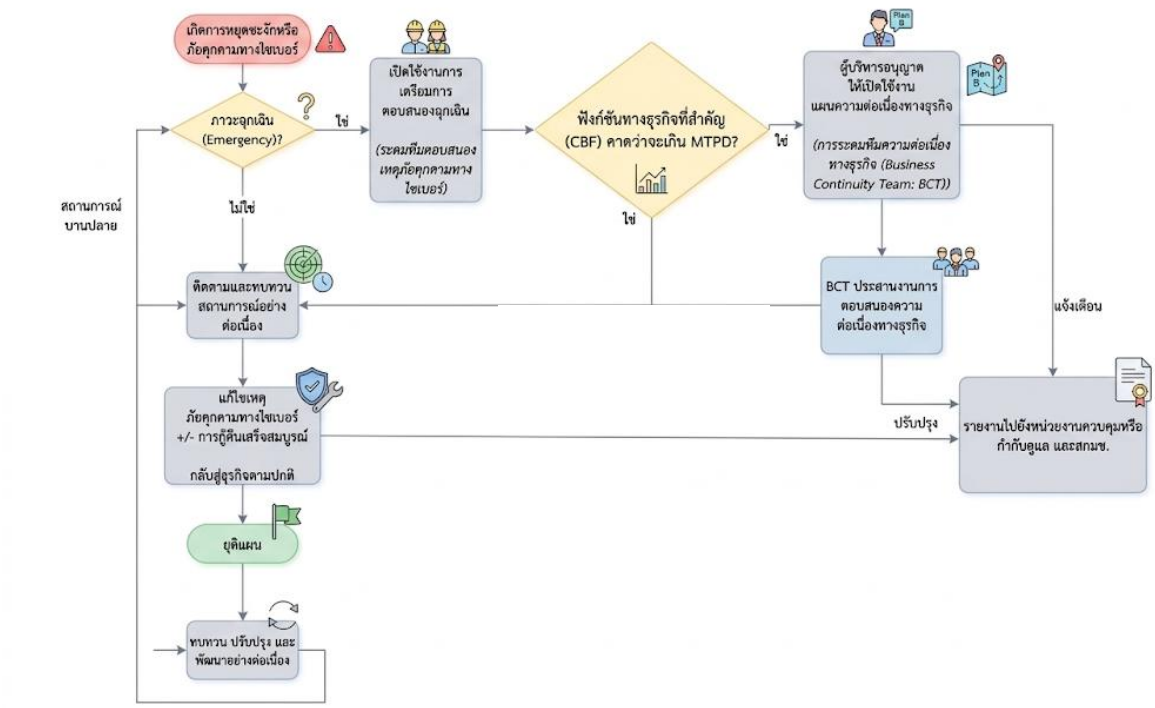
ตำแหน่งหลัก – อาคารวิทยพัฒนาชั้น ๒ จุฬาลงกรณ์มหาวิทยาลัย

สถานที่สำรองแห่งที่ ๑ - อาคารกรมส่งเสริมการค้าระหว่างประเทศ ชั้น ๑ สถาบันระหว่างประเทศเพื่อการค้าและการพัฒนา (องค์การมหาชน) รัชดา

หากสถานที่ใด ๆ ข้างต้นไม่พร้อมใช้งานหรือเหมาะสม ผู้รับผิดชอบจะใช้ดุลยพินิจในการตัดสินใจเลือกสถานที่อื่นที่ดีที่สุดสำหรับการประชุม โดยคำนึงถึงปัญหาด้านความปลอดภัยและบริเวณใกล้เคียงกับพื้นที่ที่ได้รับผลกระทบ

๗.๖ ขั้นตอนการเปิดใช้งาน (Activation Process)

ขั้นตอนต่อไปนี้สรุปความต่อเนื่องของการตอบสนองตั้งแต่เกิดการหยุดชะงัก ไปจนถึงหยุดทำงาน



รูปที่ ๓ ภาพแสดงขั้นตอนความต่อเนื่องของการตอบสนองตั้งแต่เกิดการหยุดชะงัก ไปจนถึงหยุดทำงาน

๗.๗ การยุติแผน

แผนนี้สามารถหยุดได้ เมื่อตรงตามเกณฑ์ต่อไปนี้

- ดำเนินฟังก์ชันทางธุรกิจที่สำคัญ (CBFs) ในขั้นตอนทางธุรกิจได้ตามปกติ
- ความพยายามในการกู้คืนเสร็จสิ้นแล้ว หรือภาวะหยุดชะงักได้รับการแก้ไขแล้ว

เมื่อกระบวนการทางธุรกิจตามปกติกลับมาทำงานอีกครั้ง บริการของสถาบันควรแจ้งให้ผู้มีส่วนได้ส่วนเสียที่เกี่ยวข้องทราบทั้งหมด ตามกลยุทธ์การสื่อสาร

๘. การตอบสนองของสถาบัน

ทีมความต่อเนื่องทางธุรกิจ (BCT) มีหน้าที่รับผิดชอบในการประสานงานการตอบสนองทางยุทธวิธีและการปฏิบัติงานในสถานที่เมื่อเปิดใช้งานแผนบริหารความต่อเนื่องทางธุรกิจเพื่อตอบสนองต่อการหยุดชะงัก ความรับผิดชอบหลักของทีม

๑) รวบรวมรายละเอียดและประเมินผลกระทบของเหตุภัยคุกคามทางไซเบอร์
๒) ดูแลการกลับมาเริ่มต้นใหม่ (Resumption) ของการให้บริการทางธุรกิจที่สำคัญ
๓) ติดต่อประสานงานกับบริการฉุกเฉินในท้องถิ่น สถาบันอื่น ๆ และสถาบันสนับสนุน
๔) ประสานงานการปรับใช้ทรัพยากรภายในและภายนอกที่จำเป็นเพื่อสนับสนุนการเริ่มต้นบริการใหม่และการกู้คืน
๕) ให้ผู้บริหารประเมินเหตุภัยคุกคามทางไซเบอร์และสถานะของการกู้คืน
๖) ดำเนินการทบทวนหลังเหตุภัยคุกคามทางไซเบอร์ (Post-Incident Review) และการกู้คืนระยะยาว (Long Term Recovery) (กลับสู่ภาวะปกติ)

ตารางที่ ๓ ตารางการกำหนดหน้าที่รับผิดชอบการประสานงาน

เรื่อง	บทบาท	หน้าที่และความรับผิดชอบ	รายงานต่อไปยัง
๑. การประเมินผลกระทบของเหตุ	ติดต่อประสานงาน (ปวิธ และสาธิต)	รวบรวมรายละเอียดและประเมินผลกระทบของเหตุภัยคุกคามทางไซเบอร์	DCIO และ CIO เพื่อสั่งการผู้รับผิดชอบและหรือบริษัทที่รับผิดชอบดูแลระบบ
๒. ดูแลการกลับมาเริ่มต้นใหม่ (Resumption)	ติดต่อประสานงาน (ปวิธ และสาธิต)	ดูแลการกลับมาเริ่มต้นใหม่ (Resumption) ของการให้บริการทางธุรกิจที่สำคัญ	DCIO และ CIO เพื่อสั่งการผู้รับผิดชอบและหรือบริษัทที่รับผิดชอบดูแลระบบ
๓. การใช้ทรัพยากร	ติดต่อประสานงาน (ปวิธ และสาธิต)	ปรับใช้ทรัพยากรภายในและภายนอกที่จำเป็นเพื่อสนับสนุนการเริ่มต้นบริการใหม่และการกู้คืน	DCIO และ CIO เพื่อสั่งการผู้รับผิดชอบและหรือบริษัทที่รับผิดชอบดูแลระบบ
๔. ประเมินเหตุภัยคุกคามทางไซเบอร์และสถานะของการกู้คืน	ติดต่อประสานงาน (ปวิธ และสาธิต)	บริหารประเมินเหตุภัยคุกคามทางไซเบอร์และสถานะของการกู้คืน	DCIO และ CIO
๕. การทบทวนเหตุการณ์	ติดต่อประสานงาน (ปวิธ และสาธิต)	ดำเนินการทบทวนหลังเหตุภัยคุกคามทางไซเบอร์ (Post-Incident Review) และการกู้คืนระยะยาว (Long Term Recovery) (กลับสู่ภาวะปกติ)	DCIO และ CIO เพื่อสั่งการผู้รับผิดชอบและหรือบริษัทที่รับผิดชอบดูแลระบบ

๙. กลยุทธ์การสื่อสาร

ในกรณีที่เกิดการหยุดชะงัก จำเป็นอย่างยิ่งที่ผู้มีส่วนได้ส่วนเสียจะต้องมีส่วนร่วมอย่างมีประสิทธิภาพและตระหนักถึงการหยุดชะงักและกลยุทธ์ความต่อเนื่องทางธุรกิจที่เกี่ยวข้องที่มีอยู่

โดยนักเทคโนโลยีสารสนเทศ เจ้าหน้าที่และหรือบริษัทที่ได้รับการแต่งตั้งจากสถาบันมีหน้าที่รับผิดชอบในการดำเนินการตามกลยุทธ์การสื่อสาร

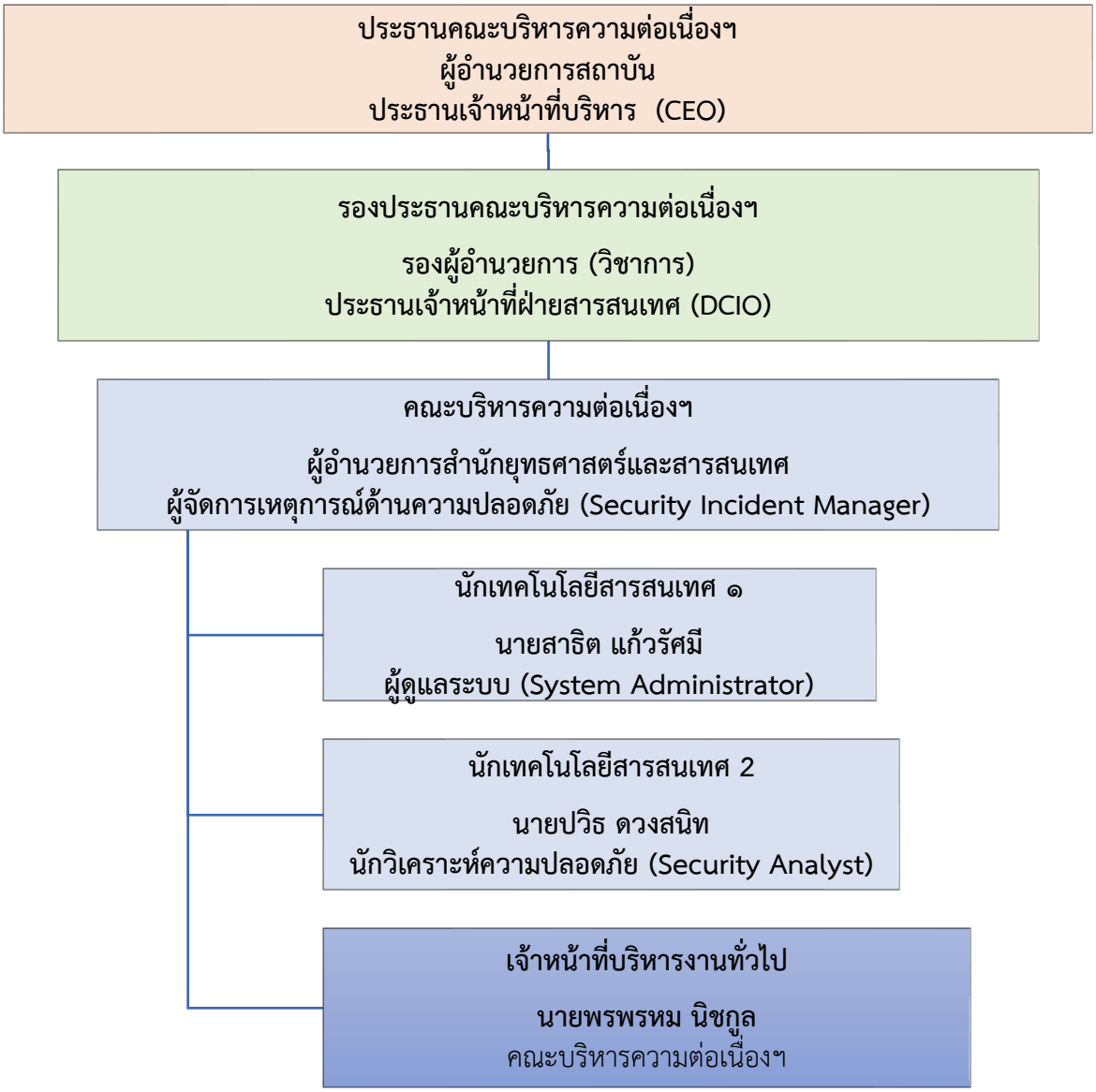
ตารางที่ ๔ การสื่อสารกับผู้มีส่วนได้ส่วนเสียที่เกี่ยวข้อง

ผู้มีส่วนได้ส่วนเสีย (Stakeholder)	วิธีการสื่อสาร	ความถี่	หมายเหตุ
เจ้าหน้าที่ภายใน	อีเมลภายใน หรือ กระดานแจ้งข่าวสาร (Forum) ให้ พนักงาน	วันละสองครั้ง รายวัน	หลังจากผ่านไปหนึ่งสัปดาห์ ให้พิจารณาอีเมลภายในวันละครั้ง และกระดานแจ้งข่าวสารให้พนักงานวันละสองครั้ง
ซัพพลายเออร์	โทรศัพท์ อีเมล	เมื่อเกิดเหตุการณ์ รายวัน	แจ้งซัพพลายเออร์เกี่ยวกับการหยุดชะงักเบื้องต้นทางโทรศัพท์ สามารถส่งการอัปเดตในภายหลังได้ทางอีเมล
สื่อสารองค์กร	แถลงข่าว แจ้งผู้มีส่วนเกี่ยวข้อง ผ่านช่องทางของสถาบัน	เมื่อเกิดเหตุการณ์ เมื่อสิ้นสุดเหตุการณ์ ตามความจำเป็น	โฆษกที่รับการแต่งตั้งควรเป็นผู้สนับสนุนผู้บริหาร

ในการแก้ปัญหาการหยุดชะงัก นักเทคโนโลยีสารสนเทศ เจ้าหน้าที่และหรือบริษัทที่ได้รับการแต่งตั้งจากสถาบัน มีหน้าที่รับผิดชอบในการแจ้งให้ผู้มีส่วนได้ส่วนเสียข้างต้นทราบถึงการเริ่มต้นกระบวนการทางธุรกิจตามปกติอีกครั้ง

๑๐. ภาคผนวกที่เกี่ยวกับการทำงาน ภาคผนวกด้านการทำงานอธิบายถึงบทบาทและความรับผิดชอบเฉพาะการดำเนินการที่ต้องดำเนินการ กลยุทธ์ความต่อเนื่องทางธุรกิจ และความต้องการทรัพยากรโดยแต่ละหน่วยธุรกิจเมื่อเปิดใช้งานแผนบริหารความต่อเนื่องทางธุรกิจ แม้ว่าเนื้อหาหลักของแผนบริหารความต่อเนื่องทางธุรกิจจะให้ข้อมูลที่ครอบคลุมเกี่ยวกับความต่อเนื่องของบริการของสถาบัน โดยรวมภาคผนวกนี้เน้นที่ความรับผิดชอบ ลักษณะงาน และการดำเนินการเฉพาะที่เกี่ยวข้องกับองค์ประกอบของแผนความต่อเนื่องทางธุรกิจที่ปฏิบัติได้

ภาคผนวก ๑
ทีมความต่อเนื่องทางธุรกิจและรักษาความมั่นคงปลอดภัยไซเบอร์



รูปที่ ๔ ภาพโครงสร้างของทีมความต่อเนื่องทางธุรกิจ (Business Continuity Team: BCT)

ทีมความต่อเนื่องทางธุรกิจ (Business Continuity Team: BCT)

หน้าที่และความรับผิดชอบ

๑) รวบรวมรายละเอียดและประเมินผลกระทบของเหตุภัยคุกคามทางไซเบอร์
๒) ดูแลการกลับมาเริ่มต้นใหม่ของบริการทางธุรกิจที่สำคัญ
๓) ติดต่อประสานงานกับบริการฉุกเฉินในท้องถิ่น สถาบันอื่น ๆ และสถาบันสนับสนุน
๔) ประสานงานการปรับใช้ทรัพยากรภายในและภายนอกที่จำเป็นเพื่อสนับสนุนการเริ่มต้นบริการใหม่และการกู้คืน
๕) ให้ผู้บริหารประเมินเหตุภัยคุกคามทางไซเบอร์และสถานะของการกู้คืน
๖) ดำเนินการทบทวนหลังเหตุภัยคุกคามทางไซเบอร์และการกู้คืนระยะยาว (กลับสู่ภาวะปกติ)

ทีมรักษาความมั่นคงปลอดภัยไซเบอร์

บทบาทและความรับผิดชอบ (Roles and Responsibilities)

๑. ประธานเจ้าหน้าที่บริหาร (CEO): (ผู้อำนวยการสถาบัน)

๑) กำหนดวิสัยทัศน์และกลยุทธ์ด้านความปลอดภัยทางไซเบอร์ขององค์กร
๒) สนับสนุนและผลักดันให้มีการลงทุนในด้านความปลอดภัยทางไซเบอร์อย่างเหมาะสม
๓) สร้างวัฒนธรรมองค์กรที่ตระหนักถึงความสำคัญของความปลอดภัยทางไซเบอร์

๒. ประธานเจ้าหน้าที่ฝ่ายสารสนเทศ (DCIO): รองผู้อำนวยการ (วิชาการ)

๑) วางแผนและบริหารจัดการระบบเทคโนโลยีสารสนเทศขององค์กรให้มีความปลอดภัย
๒) กำกับดูแลและประเมินผลการดำเนินงานด้านความปลอดภัยทางไซเบอร์
๓) รายงานสถานะและปัญหาด้านความปลอดภัยทางไซเบอร์ต่อผู้บริหารระดับสูง

๓. ผู้ดูแลระบบ (System Administrator): (นักเทคโนโลยีสารสนเทศ)

๑) ติดตั้งและบำรุงรักษาระบบคอมพิวเตอร์และเครือข่ายให้มีความปลอดภัย
๒) ตรวจสอบและแก้ไขช่องโหว่ด้านความปลอดภัย
๓) ป้องกันและแก้ไขปัญหาที่เกิดจากภัยคุกคามทางไซเบอร์

๔. นักวิเคราะห์ความปลอดภัย (Security Analyst): (นักเทคโนโลยีสารสนเทศ)

๑) ตรวจสอบและวิเคราะห์ภัยคุกคามทางไซเบอร์
๒) พัฒนาและปรับปรุงระบบป้องกัน
๓) ตอบสนองต่อเหตุการณ์ด้านความปลอดภัยทางไซเบอร์

๕. ผู้จัดการเหตุการณ์ด้านความปลอดภัย (Security Incident Manager): (ผู้อำนวยการสำนักยุทธศาสตร์และสารสนเทศ)

๑) บริหารจัดการเหตุการณ์ด้านความปลอดภัยทางไซเบอร์
๒) ประสานงานกับสถาบันที่เกี่ยวข้อง
๓) วิเคราะห์และประเมินผลกระทบจากเหตุการณ์

๑. สมาชิกในทีมความต่อเนื่องทางธุรกิจ (Business Continuity Team Members)

ตารางที่ ๕ รายชื่อสมาชิกในทีม (Team Members)

บทบาท (Role)	บุคลากรหลัก (Primary)	บุคลากรสำรอง (Alternate)
ประธานคณะบริหารความต่อเนื่องฯ ประธานเจ้าหน้าที่บริหาร (CEO)	นายสุภกิจ เจริญกุล ผู้อำนวยการ	นายวิมล ปั้นคง รองผู้อำนวยการ (วิชาการ)
รองประธานคณะบริหารความต่อเนื่องฯ ประธานเจ้าหน้าที่ฝ่ายสารสนเทศ (CIO)	นายวิมล ปั้นคง รองผู้อำนวยการ (วิชาการ)	
หัวหน้าคณะบริหารความต่อเนื่องฯ ผู้จัดการเหตุการณ์ด้านความปลอดภัย (Security Incident Manager)	นางสาวสุชาดา จังรัสสะ	
คณะบริหารความต่อเนื่องฯ ผู้ดูแลระบบ (System Administrator) และ นักวิเคราะห์ความปลอดภัย (Security Analyst)	นายสาธิต แก้วรัศมี นักเทคโนโลยีสารสนเทศอาวุโส	
คณะบริหารความต่อเนื่องฯ ผู้ดูแลระบบ (System Administrator) และ นักวิเคราะห์ความปลอดภัย (Security Analyst)	นายปวิธ ดวงสนิท นักเทคโนโลยีสารสนเทศอาวุโส	
คณะบริหารความต่อเนื่องฯ	นายพรพรหม นิชกูล เจ้าหน้าที่บริหารงานทั่วไป	

๒. จุดควบคุมเหตุภัยคุกคามทางไซเบอร์ (Incident Control Point)

ตารางที่ ๖ จุดควบคุมเหตุภัยคุกคามทางไซเบอร์ (Incident Control Point)

สถานที่หลัก (Primary location)	อาคารวิทยพัฒนาชั้น ๒ จุฬาลงกรณ์มหาวิทยาลัย
สถานที่สำรองแห่งที่ ๑ (๑st alternate location)	อาคารกรมส่งเสริมการค้าระหว่างประเทศ ชั้น ๑ สถาบันระหว่างประเทศเพื่อการค้าและการพัฒนา (องค์การมหาชน) รัชดา

๓. การดำเนินการตอบสนอง (Response Actions)

๓.๑ ตารางที่ ๗ การดำเนินการทันที (Immediate)

การดำเนินการ (Action)	ผู้รับผิดชอบ	เอกสารอ้างอิง (Reference)
☐ เริ่มต้นบันทึกเหตุภัยคุกคามทางไซเบอร์ (Initiate Incident Log)	นายสาธิต แก้วรัศมี นักเทคโนโลยีสารสนเทศอาวุโส	
☐ รับรายงานสถานการณ์ทั่วไปจากผู้แจ้ง (Obtain General Situation Report From the Notifier)	นายปวิธ ดวงสนิท นักเทคโนโลยีสารสนเทศอาวุโส	
☐ แจ้งสมาชิกคนอื่น ๆ ในทีมตามที่จำเป็น (Notify other Members of the Team as Required)	นายพรพรหม นิชกูล เจ้าหน้าที่บริหารงานทั่วไป	
☐ กำหนดลักษณะของเหตุภัยคุกคามทางไซเบอร์ (Determine the Nature of the Incident) ๑) เกิดอะไรขึ้น? (What has happened?) ๒) มีใครบาดเจ็บหรือไม่? (Is anyone hurt?) ๓) บริการ / พื้นที่ใดบ้างที่ได้รับผลกระทบ (What Services / areas are affected?) ๔) ผลกระทบต่อกิจกรรม/บริการทางธุรกิจที่สำคัญอะไร? (What is the impact on critical business activities / services?) ๕) ทำอะไรไปแล้วบ้าง? (What has been done?) ๖) การหยุดชะงักมีแนวโน้มที่จะคงอยู่นานแค่ไหน? (How long is the disruption likely to last?)	หัวหน้าคณะบริหารความต่อเนื่องฯ	

๓.๒ การดำเนินการต่อเนื่อง (On-going)

ตารางที่ ๘ แบบตารางการดำเนินการต่อเนื่องของสถาบัน

การดำเนินการ	ผู้รับผิดชอบ	หมายเหตุ/ เอกสารอ้างอิง
☐ ติดตามผลการดำเนินการที่เกี่ยวข้อง	ประธานคณะบริหารความต่อเนื่องฯ (ผู้อำนวยการสถาบัน)	

การดำเนินการ	ผู้รับผิดชอบ	หมายเหตุ/ เอกสารอ้างอิง
☐ รายงานผลการดำเนินการและแจ้งเหตุที่เกิดขึ้น	หัวหน้าคณะบริหารความต่อเนื่องฯ (ผู้อำนวยการสำนักยุทธศาสตร์)	

๓.๓ การดำเนินการหลังเหตุภัยคุกคามทางไซเบอร์ (Post-incident)

ตารางที่ ๙ การดำเนินการหลังเหตุภัยคุกคามทางไซเบอร์ของสถาบัน

การดำเนินการ	ผู้รับผิดชอบ	หมายเหตุ/ เอกสารอ้างอิง
☐ รวบรวมบันทึกเหตุการณ์ ข้อมูลล็อก และหลักฐานดิจิทัลอื่น ๆ ที่เกี่ยวข้องกับการโจมตี	นายสาธิต แก้วรัศมี นักเทคโนโลยีสารสนเทศอาวุโส	
☐ วิเคราะห์หลักฐานเพื่อระบุสาเหตุของการโจมตี วิธีการที่ผู้โจมตีใช้ และประเมินความเสียหายที่เกิดขึ้นกับระบบข้อมูล และธุรกิจ	นายปวิธ ดวงสนิท นักเทคโนโลยีสารสนเทศอาวุโส	
☐ เก็บรักษาหลักฐานอย่างปลอดภัยสำหรับการตรวจสอบในอนาคตหรือการดำเนินคดีตามกฎหมาย	นายสาธิต แก้วรัศมี นักเทคโนโลยีสารสนเทศอาวุโส	
☐ แก้ไขจุดอ่อนในระบบรักษาความปลอดภัยที่ถูกค้นพบ และหรือ การอัปเดตซอฟต์แวร์ และระบบต่าง ๆ ให้มีความทันสมัยอยู่เสมอ	นายปวิธ ดวงสนิท นักเทคโนโลยีสารสนเทศอาวุโส	
☐ ปรับปรุงนโยบายและขั้นตอนการรักษาความปลอดภัยให้ครอบคลุมและมีประสิทธิภาพยิ่งขึ้น	นายปวิธ ดวงสนิท นักเทคโนโลยีสารสนเทศอาวุโส	
☐ จัดทำรายงานสรุปเหตุการณ์ ผลการวิเคราะห์ และมาตรการปรับปรุง	นายสาธิต แก้วรัศมี นักเทคโนโลยีสารสนเทศอาวุโส	
☐ รายงานเหตุการณ์ไปยังผู้บริหาร สถาบันกำกับดูแล หรือสถาบันบังคับใช้กฎหมายที่เกี่ยวข้อง (หากจำเป็น)	นายปวิธ ดวงสนิท นักเทคโนโลยีสารสนเทศอาวุโส	

๔. รายชื่อผู้ติดต่อ

ตารางที่ ๑๐ การติดต่อภายใน

บทบาท	ชื่อ	โทรศัพท์ ในเวลาทำงาน #	โทรศัพท์ นอกเวลาทำงาน #	อีเมล
ติดตามรายงานและแก้ไขปรับปรุง	นายสาธิต แก้วรัศมี	๐๒ ๒๑๖ ๑๘๙๔-๗ #๑๕๒	๐๖๒ ๔๙๔ ๔๙๑๔	satit@itd.or.th
ติดตามรายงานและแก้ไขปรับปรุง	นายปวิธ ดวงสนิท	๐๒ ๒๑๖ ๑๘๙๔-๗ #๑๕๕	๐๘๖ ๙๙๖ ๓๓๒๕	pawith@itd.or.th

ตารางที่ ๑๑ การติดต่อภายนอก

สถาบัน/บริษัท	การให้บริการ/สนับสนุน	ข้อมูลการติดต่อ ๑		ข้อมูลการติดต่อ ๒
บริษัท มณฑรัตน์ เทรดดิ้ง จำกัด	ltd.or.th	Name	นายอนิรุทธ์ รอดเที่ยง	นายศุภณัฐ บุญสารี
		Position	ผู้ดูแลระบบ	ผู้ดูแลระบบ
		E-mail	t๒eaway@gmail.com	thana๑๐๓@gmail.com
		Tel	๐๘๖ ๔๕๕ ๖๑๔๐	๐๙๐ ๒๘๖ ๐๔๕๔
		Office Hours #	๐๙.๐๐ น.	๐๙.๐๐ น.
		After Hours #	๑๘.๐๐ น.	๑๘.๐๐ น.
บริษัท เท็คไอทีโซลูชั่น จำกัด	ระบบสารสนเทศในการบริหารจัดการองค์กร ด้านงบประมาณ การเงิน บัญชี และวัสดุ (e-Budget)	Name	นางสาวรัชวิชา รอบจังหวัด	นายปัณณวิทชญ์ เอกอาภาปะเสริฐ
		Position	Project Manager	Assistant System Analyst
		E-mail	ratchawicha@takeitsolution.com	Punnavit.e@takeitsolution.com
		Tel	๐๘๑ ๕๖๒ ๔๒๖๔	๐๖๒ ๒๕๔ ๑๗๔๖๓
		Office Hours #	๐๙.๐๐ น.	๐๙.๐๐ น.
		After Hours #	๑๘.๐๐ น.	๑๘.๐๐ น.
บริษัท เวิร์คโมชั่น จำกัด	ระบบ Prompt Pass	Name	นายเปรมินทร์ บัวพิณ	นางสาวบุญสิตา เมฆแจ้ง
		Position	ผู้จัดการโครงการ	ผู้ช่วยผู้จัดการโครงการ
		E-mail	zo.workmotion@gmail.com	baitoey.workmotion@gmail.com

สถาบัน/บริษัท	การให้บริการ/สนับสนุน	ข้อมูลการติดต่อ ๑		ข้อมูลการติดต่อ ๒
		Tel	๐๙๖ ๑๕๙ ๙๔๔๗	๐๙๕ ๕๖๗ ๑๖๙๐
		Office Hours #	๐๙.๐๐ น.	๐๙.๐๐ น.
		After Hours #	๑๘.๐๐ น.	๑๘.๐๐ น.
บริษัท ฮิวแมนซอฟท์ จำกัด	ระบบบุคคล Humansoft	Name	นางสาวชัชภรณ์ อัศดรไพรศานติ์	
		Position	ฝ่ายขาย	
		E-mail	sale@humansoft.co.th	
		Tel	๐๘๐ ๔๕๓ ๔๖๘๖	
		Office Hours #	๐๙.๐๐ น.	
		After Hours #	๑๘.๐๐ น.	
สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน)	e-Office	Name	สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน)	
		Position		
		E-mail	mallika.sr@d-solution.co.th	
		Tel	๐๒ ๖๑๒ ๖๐๖๐	
		Office Hours #	๘.๐๐ น.	
		After Hours #	๑๖.๐๐ น.	

สถาบัน/บริษัท	การให้บริการ/สนับสนุน	ข้อมูลการติดต่อ ๑		ข้อมูลการติดต่อ ๒
บริษัท ซีเอส ล็อกซอินโฟ จำกัด (มหาชน)(CS Loxinfo Public Company Limited)	เว็บไซต์ BCGconnex	Name	นางสาวพิมพ์ศิรี ทิพยนารถ	
		Position	Senior Business Development	
		E-mail	pimsiret@ais.co.th	
		Tel	๐๒ ๒๖๓ ๘๐๐๐	
		Office Hours #	๐๙.๐๐ น.	
		After Hours #	๑๘.๐๐ น.	

๒. ฟังก์ชันที่สำคัญ (Critical Functions)

ตารางที่ ๑๒ ฟังก์ชันที่สำคัญ (Critical Functions) ของสถาบัน

หน่วยธุรกิจ (Business Unit)	กิจกรรม/ฟังก์ชั่น (Activity/ Function)	Maximum Tolerable Downtime: MTD)					
		๘ hrs	๑ day	๓ days	๑ wk	๒ wks	≥๑ month
เว็บไซต์ ltd.or.th	ระบบเว็บไซต์สถาบัน			✓			
เว็บไซต์ BCGconnex	ระบบเว็บไซต์ BCG			✓			
ระบบสารสนเทศในการบริหารจัดการองค์กร ด้านงบประมาณ การเงิน บัญชี และวัสดุ (e-Budget)	ระบบบริหารบัญชีงบประมาณ			✓			
ระบบ Prompt Pass	ระบบคลินิกเสมือนจริง SMEs			✓			
เว็บไซต์ Prompt Pass	เว็บไซต์ Prompt Pass			✓			
ระบบบริหารจัดการสำนักงาน (e-Office)	ระบบบริหารจัดการสำนักงาน			✓			
ระบบบุคคล Humansoft	ระบบบริหารจัดการบุคคล			✓			

๓. กลยุทธ์ความต่อเนื่องทางธุรกิจ (Business Continuity Strategies)

ตารางที่ ๑๓ กลยุทธ์ความต่อเนื่องทางธุรกิจ (Business Continuity Strategies) ต่อระบบของสถาบัน

กิจกรรม/ฟังก์ชั่น (Activity/ Function)	กลยุทธ์ความต่อเนื่องที่ดำเนินการทันที (Immediate Continuity Strategy)	ระยะเวลาเป้าหมายในการฟื้นฟู (Recovery Time Objective)	กลยุทธ์ความต่อเนื่องที่ยั่งยืน (Sustainable Continuity Strategy)	ระบบนี้ล่มได้นานที่สุด (Maintainable Duration)
ระบุความเสี่ยงที่อาจเกิดขึ้นและส่งผลกระทบต่อธุรกิจ	ประเมินผลกระทบและความน่าจะเป็นของแต่ละความเสี่ยง	๑๒ ชม.	๒๔ ชม.	๗๒ ชม.

กิจกรรม/ฟังก์ชั่น (Activity/ Function)	กลยุทธ์ความต่อเนื่องที่ดำเนินการทันที (Immediate Continuity Strategy)	ระยะเวลาเป้าหมายในการฟื้นฟู (Recovery Time Objective)	กลยุทธ์ความต่อเนื่องที่ยั่งยืน (Sustainable Continuity Strategy)	ระบบนี้ล่มได้นานที่สุด (Maintainable Duration)
ระบุกระบวนการและทรัพยากรที่สำคัญต่อการดำเนินธุรกิจ	ระบุกระบวนการและทรัพยากรที่สำคัญต่อการดำเนินธุรกิจ	๑๒ ชม.	๒๔ ชม.	๗๒ ชม.
กำหนดกลยุทธ์และแผนการดำเนินงานเพื่อรับมือกับแต่ละความเสี่ยง	กำหนดกลยุทธ์และแผนการดำเนินงานเพื่อรับมือกับแต่ละความเสี่ยง	๒๔ ชม.	๒๔ ชม.	๗๒ ชม.
จัดทำเอกสารที่รวบรวมรายละเอียดของกลยุทธ์และแผนการดำเนินงาน	จัดทำเอกสารที่รวบรวมรายละเอียดของกลยุทธ์และแผนการดำเนินงาน	๑๒ ชม.	๒๔ ชม.	๔๘ ชม.
ทดสอบแผนความต่อเนื่องทางธุรกิจอย่างสม่ำเสมอ	ทดสอบแผนความต่อเนื่องทางธุรกิจอย่างสม่ำเสมอ	๒๔ ชม.	๒๔ ชม.	๒๔ ชม.

๔. การดำเนินการตอบสนอง (Response Actions)

ตารางที่ ๑๔ การดำเนินการทันที (Immediate)

การดำเนินการ (Action)	ผู้รับผิดชอบ	เอกสารอ้างอิง (Reference)
☐ เริ่มต้นบันทึกเหตุภัยคุกคามทางไซเบอร์ (Initiate Incident Log)	นายสาธิต แก้วรัศมี นายปวิธ ดวงสนิท	
☐ รับรายงานสถานการณ์ทั่วไปจากผู้แจ้ง (Obtain General Situation Report from the Notifier)	นายสาธิต แก้วรัศมี นายปวิธ ดวงสนิท	
☐ แจ้งสมาชิกคนอื่น ๆ ในทีมตามที่จำเป็น (Notify Other Members of the Team as Required)	นายสาธิต แก้วรัศมี นายปวิธ ดวงสนิท	
☐ กำหนดลักษณะของเหตุภัยคุกคามทางไซเบอร์ (Determine the Nature of the Incident) เกิดอะไรขึ้น? (What has happened?)	นายสาธิต แก้วรัศมี นายปวิธ ดวงสนิท	

การดำเนินการ (Action)	ผู้รับผิดชอบ	เอกสารอ้างอิง (Reference)
มีใครบาดเจ็บหรือไม่? (Is anyone hurt?) บริการ / พื้นที่ใดบ้างที่ได้รับผลกระทบ? (What services/ areas are affected?) ผลกระทบต่อกิจกรรม/บริการทางธุรกิจที่สำคัญอะไร? (What is the impact on critical Business Activities/ Services?) ทำอะไรไปแล้วบ้าง? (What has been done?) การหยุดชะงักมีแนวโน้มที่จะคงอยู่นานแค่ไหน? (How long is the disruption likely to last?)		
☐ กำหนดแผนสำหรับการดำเนินกลยุทธ์ความต่อเนื่องในทันทีสำหรับหน้าที่ทางธุรกิจที่สำคัญ (Formulate Plan for Carrying out Immediate Continuity Strategy for Critical Business Functions)	นายวิมล ปั้นคง	
☐ ตัดสินใจว่าพนักงานควรอยู่ที่เดิม กลับบ้าน หรือย้ายไปที่ไซต์อื่น (Decide if staff should remain where they are, go home or relocate to the alternate site)	นายสุภกิจ เจริญกุล	

ตารางที่ ๑๕ การดำเนินการต่อเนื่อง (On-going)

การดำเนินการ (Action)	ผู้รับผิดชอบ	เอกสารอ้างอิง (Reference)
☐ ประสานงานโดยสื่อสารอย่างต่อเนื่องกับผู้มีส่วนได้ส่วนเสีย (Coordinate on-going Communications with Stakeholders)	นายสาธิต แก้วรัศมี นายปวิธ ดวงสนิท	
☐ ดูแลความปลอดภัยและสวัสดิภาพของบุคลากรทุกคน (Ensure safety and Wellbeing of all Personnel)	นายสาธิต แก้วรัศมี นายปวิธ ดวงสนิท	
☐ ตั้งค่ารายชื่อสำหรับการหมุนเวียนสมาชิกในทีมหากเหตุการณ์ยืดเยื้อ (Set up Roster for Rotation of Team Members if Incident is Prolonged)	นายภานุมาส เทพทอง	
☐ ประสานงานกับทีมจัดการเหตุฉุกเฉิน (Emergency Management Team: EMT) เพื่อปรับใช้ทรัพยากรเพิ่มเติมเพื่อสนับสนุนการกู้คืน (Liaise with EMT for Deployment of Additional Resources to Support Recovery)	นายสาธิต แก้วรัศมี นายปวิธ ดวงสนิท	
☐ ให้การอัปเดต EMT เป็นประจำ (Provide Regular Updates to the EMT)	นายสาธิต แก้วรัศมี นายปวิธ ดวงสนิท	
☐ กำหนดแผนสำหรับการใช้กลยุทธ์ความต่อเนื่องอย่างยั่งยืนสำหรับฟังก์ชันทางธุรกิจที่สำคัญ หากจำเป็น(Formulate	นายวิมล ปั้นคง	

การดำเนินการ (Action)	ผู้รับผิดชอบ	เอกสารอ้างอิง (Reference)
Plan for Implementing Sustainable Continuity Strategy for Critical Business Functions, if Necessary)		

ตารางที่ ๑๖ การดำเนินการหลังเหตุภัยคุกคามทางไซเบอร์ (Post-Incident)

การดำเนินการ (Action)	ผู้รับผิดชอบ	เอกสารอ้างอิง (Reference)
☐ เตรียมแผนยุติการดำเนินการของทีม (Prepare Plan for Standing Down the Team)	นางสาวสุชาดา จังรัสสะ	
☐ ประสานงานกับ EMT ในการยุติการดำเนินการของทีม (Liaise with EMT on Standing Down the Team)	นางสาวสุชาดา จังรัสสะ	
☐ รวบรวมบันทึกเหตุภัยคุกคามทางไซเบอร์และส่งไปยัง Emergency Management Team: EMT หรือทีมบริหารจัดการภาวะฉุกเฉิน (Collect Incident Logs and Submit to EMT)	นายสาธิต แก้วรัศมี นายปวิธ ดวงสนิท	
☐ ดำเนินการบรรยายสรุปร่วมกับทีม (Conduct debrief with Team)	นางสาวสุชาดา จังรัสสะ	
☐ หากจำเป็น มอบหมายเจ้าหน้าที่ให้เข้าร่วมทีมกู้คืนระยะยาว (Assign Staff to Participate in Long Team Recovery Team, if Necessary)	นายสุภกิจ เจริญกุล นายวิมล ปั้นคง	
☐ กำหนดแผนสำหรับฟื้นฟูความเสียหายที่เกิดจากภัยคุกคามทางไซเบอร์สำหรับฟังก์ชันทางธุรกิจที่ไม่สำคัญ (Formulate Plan for Resuming Non-critical Business Functions)	นายวิมล ปั้นคง	

๕. ความต้องการทรัพยากร (Resource Requirements)

ตารางที่ ๑๗ ตารางความต้องการทรัพยากรบุคลากร (People)

ความต้องการทรัพยากร (Resource Requirements)	ตำแหน่ง (Position)	ปัจจุบัน (Current)	จำนวนที่ต้องการ (Cumulative Quantity Required)					
			๘ hrs	๑ day	๓ days	๑ wk	๒ wks	≥๑ mth
จำนวนบุคลากร (People)	ผู้ดูแลระบบ (System Administrator)	๒	๐	๐	๐	๐	๐	๒
	นักวิเคราะห์ความปลอดภัย (Security Analyst)	๐	๐	๐	๐	๐	๐	๑
	ผู้จัดการเหตุการณ์ด้านความปลอดภัย (Security Incident Manager)	๑	๐	๐	๐	๐	๐	๑
	รวมทั้งสิ้น (Total)	**๓**	๐	๐	๐	๐	๐	**๔**

ตารางที่ ๑๘ ตารางความต้องการทรัพยากร (Resource Requirements)

ความต้องการทรัพยากร (Resource Requirements)	ประเภท (Type)	ปัจจุบัน (Current)	จำนวนที่ต้องการ (Cumulative Quantity Required)					
			๘ hrs	๑ day	๓ days	๑ wk	๒ wks	≥๑ mth
๑) โทรคมนาคม (Office Equipment and Telecommunications)	Cloud Sever	๑	-	-	-	-	-	๑
๒) อุปกรณ์ทางการแพทย์ (Medical Equipment)	ยังไม่มีความจำเป็นต้องใช้งาน	๐	-	-	-	-	-	-

ความต้องการทรัพยากร (Resource Requirements)	ประเภท (Type)	ปัจจุบัน (Current)	จำนวนที่ต้องการ (Cumulative Quantity Required)					
			๘ hrs	๑ day	๓ days	๑ wk	๒ wks	≥๑ mth
๓) อุปกรณ์เฉพาะ (Specialized Equipment)	ยังไม่มีอุปกรณ์เฉพาะ	๐	-	-	-	-	-	-
๔) วัสดุสิ้นเปลืองที่สำคัญ (Key Consumables)	ยังไม่มีวัสดุสิ้นเปลือง	๐	-	-	-	-	-	-
	รวมทั้งสิ้น (Total)	๑	-	-	-	-	-	๑

ตารางที่ ๑๙ ตารางระบบ/แอปพลิเคชัน (Systems/ Applications)

ชื่อระบบ/แอปพลิเคชัน (Name of System/ Application	ระบบ/แอปพลิเคชัน ที่ต้องการ (System / Application Required)					
	๘ hrs	๑ day	๓ days	๑ wk	๒ wks	≥๑ mth
ยังไม่มีความจำเป็นต้องใช้ระบบ/แอปพลิเคชัน เพิ่มเติมในการดำเนินการตรวจสอบด้านความปลอดภัย	-	-	-	-	-	-

๖. การพึ่งพาอาศัยกัน (Interdependencies)

ตารางที่ ๒๐ ให้บริการกับฟังก์ชันการทำงานที่สำคัญ (Upstream Interdependencies)

ภายใน (Internal)	ลักษณะของการปฏิสัมพันธ์ (Nature of Interaction)
มีการนำเข้าข้อมูล	เจ้าหน้าที่หรือผู้ใช้บริการนำเข้าข้อมูลผ่านระบบคอมพิวเตอร์หรืออุปกรณ์ที่รองรับ
ภายนอก (External)	**ลักษณะของการปฏิสัมพันธ์ (Nature of Interaction)**
ระบบมีการดึงข้อมูลจากระบบคลาวด์	เจ้าหน้าที่หรือผู้ใช้บริการนำข้อมูลจากระบบผ่านระบบคอมพิวเตอร์หรืออุปกรณ์ที่รองรับ

ตารางที่ ๒๑ ใช้บริการจากฟังก์ชันการทำงานทางธุรกิจ (Downstream Interdependencies)

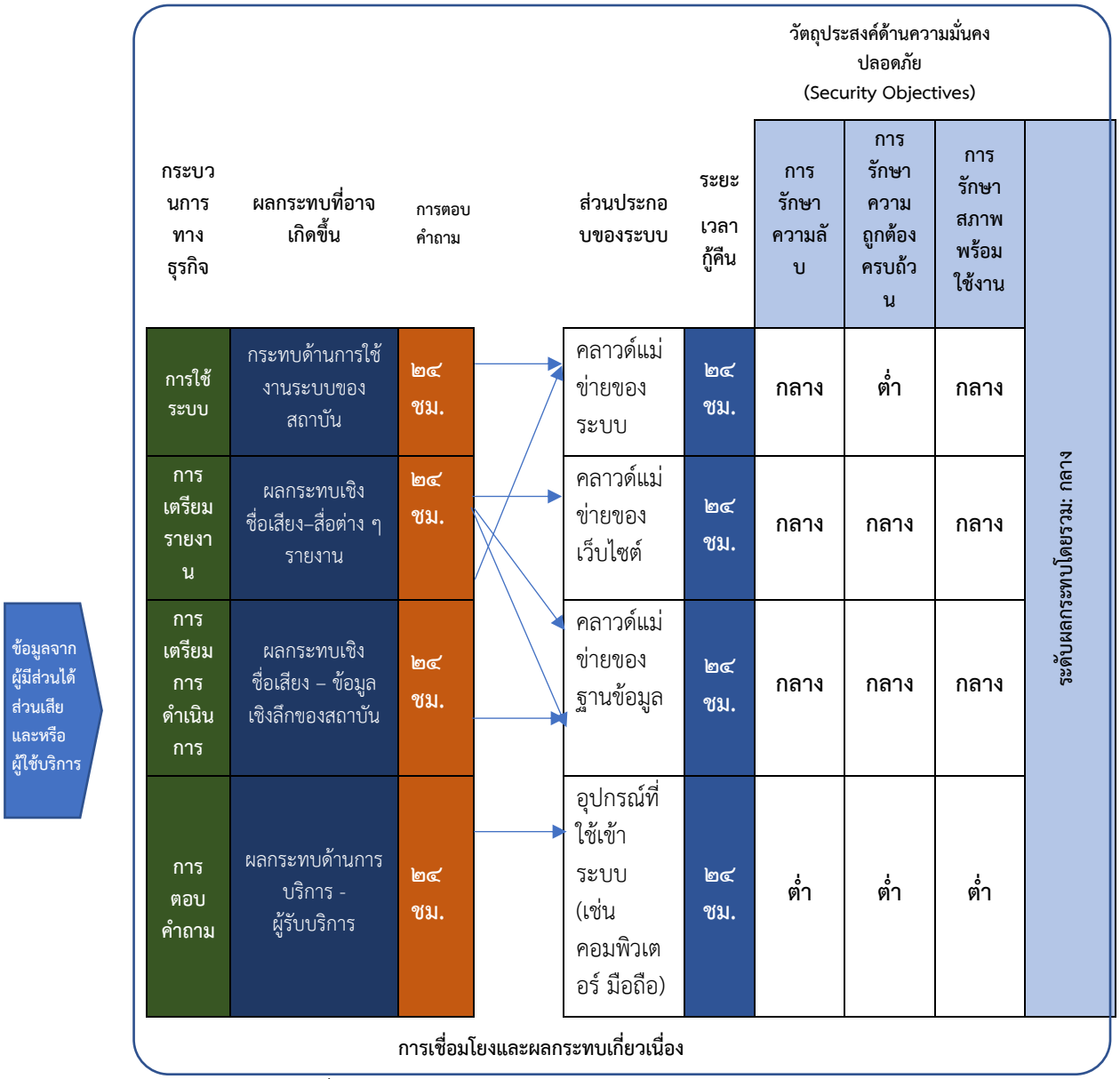
ภายใน (Internal)	ลักษณะของการปฏิสัมพันธ์ (Nature of Interaction)
ระบบมีการดึงข้อมูลจากระบบคลาวด์	เจ้าหน้าที่หรือผู้ใช้บริการนำข้อมูลจากระบบผ่านระบบคอมพิวเตอร์หรืออุปกรณ์ที่รองรับ
ภายนอก (External)	**ลักษณะของการปฏิสัมพันธ์ (Nature of Interaction)**
ระบบมีการดึงข้อมูลจากระบบคอมพิวเตอร์หรืออุปกรณ์ที่รองรับ	เมื่อผู้ใช้งานนำเข้าข้อมูลมีการดึงข้อมูลจากระบบคอมพิวเตอร์หรืออุปกรณ์ที่รองรับ ไปจัดเก็บบนระบบคลาวด์

๗. การวิเคราะห์ผลกระทบทางธุรกิจ (Business Impact Analysis: BIA)

เป็นขั้นตอนสำคัญในการกำหนดมาตรการควบคุมด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ การวิเคราะห์ดังกล่าวช่วยให้สถาบันสามารถระบุลักษณะต่าง ๆ ของส่วนประกอบของระบบสารสนเทศ รวมทั้งภารกิจหรือการดำเนินงานสำคัญของสถาบันที่ได้รับสนับสนุนจากระบบสารสนเทศดังกล่าว รวมถึงการพึ่งพาซึ่งกันและกันของระบบสารสนเทศและการดำเนินงานต่าง ๆ ของสถาบัน

๘. กระบวนการวิเคราะห์ผลกระทบทางธุรกิจ (BIA)

สถาบันสามารถดำเนินการวิเคราะห์ผลกระทบทางธุรกิจตามขั้นตอนด้านล่าง และอาจพิจารณาปรับขั้นตอนดังกล่าวให้เข้ากับบริบทของสถาบัน เพื่อให้สถาบันมั่นใจว่าการดำเนินการวิเคราะห์ผลกระทบทางธุรกิจ เป็นการดำเนินงานที่ครอบคลุมผลกระทบต่าง ๆ ที่อาจเกิดขึ้นหากบริการที่สำคัญของสถาบันหยุดชะงัก ทั้งนี้สถาบันควรวิเคราะห์ภัยคุกคามหรืออันตรายที่จะเกิดต่อการดำเนินงานที่สำคัญต่อพันธกิจของสถาบันทีละการดำเนินงาน



รูปที่ ๕ ภาพแสดงกระบวนการวิเคราะห์ผลกระทบทางธุรกิจ

ขั้นตอนที่ ๑ การกำหนดกระบวนการทางธุรกิจหรือบริการที่สำคัญต่อภารกิจของสถาบัน ระบบสารสนเทศมีจำนวนมากอาจมีความซับซ้อน เนื่องจากถูกออกแบบมาเพื่อสนับสนุนกระบวนการหรือการให้บริการที่หลากหลาย จึงเป็นไปได้ว่าบุคคลที่ได้รับบริการต่างกัน หรือบุคลากรที่มีหน้าที่รับผิดชอบดำเนินการของกระบวนการต่างกันอาจมีมุมมองต่อความสำคัญของระบบสารสนเทศเดียวกันต่างกันได้

ขั้นตอนที่ ๒ การพิจารณาผลกระทบจากการหยุดชะงักของกระบวนการหรือบริการที่สำคัญ หลังจากที่สถาบันดำเนินการในขั้นตอนที่ ๑ และได้กระบวนการทางธุรกิจหรือบริการที่สำคัญต่อภารกิจของสถาบันแล้ว ในขั้นตอนนี้สถาบันพิจารณาผลกระทบจากการหยุดชะงักของกระบวนการหรือบริการที่สำคัญที่อาจเกิดขึ้น เมื่อเกิดภัยคุกคามและอันตรายต่อระบบสารสนเทศที่เกี่ยวข้อง

ตารางที่ ๒๒ ภัยคุกคามและอันตรายที่อาจเกิดขึ้นต่อระบบสารสนเทศ

ภัยคุกคามและอันตรายจากภายนอก
• การโจมตีด้วยอาวุธ
• การโจมตีโครงสร้างพื้นฐาน เช่น ไฟฟ้าดับ ระบบการสื่อสารหยุดชะงัก การหยุดชะงักของระบบขนส่ง ความล้มเหลวของระบบระบายอากาศ การปนเปื้อนของน้ำประปา ระบบบำบัดน้ำเสียล้มเหลว
• การโจมตีทางไซเบอร์ เช่น การสูญเสียข้อมูลหรือการหยุดชะงักของบริการเครือข่าย ระบบควบคุมล้มเหลว
• การโจมตีด้านเศรษฐกิจ/แรงงาน/การจลาจล เช่น การก่อความไม่สงบ การจลาจล หายนะทางเศรษฐกิจ การประท้วงหยุดงาน
• ภัยธรรมชาติ เช่น พายุ น้ำท่วม สึนามิ ไฟป่า
ภัยคุกคามและอันตรายจากกระบวนการ
• สิ่งสนับสนุนสำคัญไม่เพียงพอ • การออกแบบกระบวนการไม่เหมาะสม • ห่วงโซ่อุปทานล้มเหลว
ภัยคุกคามและอันตรายจากภายในสถาบัน
• ภัยคุกคามจากภายในสถาบัน • การวางแผนที่ไม่ดี • ระบบไอทีล่ม • ความล้มเหลวในการรับรู้ข้อกำหนด/อุปสรรค

ขั้นตอนที่ ๓ การประเมินเวลาการหยุดชะงักที่ยอมรับได้ หลังจากนั้นสถาบันควรใช้ผลจากการพิจารณาผลกระทบในขั้นตอนที่ ๒ เพื่อกำหนดระยะเวลาที่ระบบต้องหยุดชะงักลง (Downtime) ร่วมกับเจ้าของกระบวนการ (Process Owner) ผู้บริหาร และผู้จัดการที่เกี่ยวข้องกับธุรกิจ (Business Manager) สถาบันสามารถกำหนดระยะเวลาได้ ๓ ช่วงเวลา

ขั้นตอนที่ ๔ การระบุข้อกำหนดด้านทรัพยากร ระบบสารสนเทศบางระบบมีความสำคัญต่อการดำเนินธุรกิจหรือบริการที่สำคัญอันเป็นภารกิจของสถาบัน การประเมินทรัพยากรของระบบดังกล่าวอย่างละเอียดจึงเป็นกุญแจสำคัญในการกู้คืนการดำเนินการหรือบริการที่สำคัญของสถาบันอย่างมีประสิทธิภาพ

ขั้นตอนที่ ๕ การกำหนดลำดับความสำคัญของทรัพยากรของระบบสารสนเทศ การกำหนดลำดับความสำคัญในการกู้คืนเป็นขั้นตอนสุดท้ายของกระบวนการวิเคราะห์ผลกระทบทางธุรกิจ

๙. การวิเคราะห์ผลกระทบทางธุรกิจ (BIA)

๙.๑ การกำหนดกระบวนการทางธุรกิจหรือบริการที่สำคัญต่อภารกิจของสถาบัน

ตารางด้านล่างนี้ เป็นเครื่องมือช่วยในการรวบรวมข้อมูลจากผู้ใช้งาน ผู้จัดการ เจ้าของกระบวนการทางธุรกิจ และผู้ประสานงานที่เกี่ยวข้องกับระบบสารสนเทศ เพื่อระบุกระบวนการทางธุรกิจที่มีการพึ่งพาหรือใช้ในการสนับสนุนระบบสารสนเทศอื่น

ตารางที่ ๒๓ การกำหนดกระบวนการทางธุรกิจ

กระบวนการทางธุรกิจ	คำอธิบาย
ระบบเว็บไซต์สถาบัน โดเมนเนม itd.or.th	ขั้นตอนทางสืบค้นงานวิจัย การสมัครเข้าร่วมกิจกรรมประชุม อบรม สัมมนาทางอิเล็กทรอนิกส์ และการยืนยันการรับสมัครเข้าร่วมกิจกรรม
ระบบเว็บไซต์สถาบัน โดเมนเนม BCGconnex.com	ระบบทางสืบค้นผู้ประกอบการ เชื่อมโยงผู้ประกอบการ SMEs การสมัครเข้าร่วมกิจกรรมประชุม อบรม สัมมนา ผู้ประกอบการ BCG จับคู่ผู้ค้า
ระบบสารสนเทศในการบริหารจัดการองค์กร ด้านงบประมาณ การเงิน บัญชี และวัสดุ (e-Budget)	ระบบที่ใช้ในการบริหารจัดการเงินงบประมาณขององค์กรหรือสถาบัน วางแผนกำหนดการใช้จ่าย ควบคุมติดตามการใช้จ่ายตามแผน บันทึกเก็บข้อมูลรายรับรายจ่าย รายงานแสดงผลการเงิน
ระบบ Prompt Pass	ระบบสืบค้นผู้เชี่ยวชาญ การสมัครเข้าร่วมกิจกรรมประชุม อบรม สัมมนาทางอิเล็กทรอนิกส์ และการรับคำปรึกษาออนไลน์
ระบบคลาวด์เว็บ Prompt Pass	ระบบสืบค้นผู้เชี่ยวชาญ การสมัครเข้าร่วมกิจกรรมประชุม อบรม สัมมนาทางอิเล็กทรอนิกส์ และการรับคำปรึกษาออนไลน์
ระบบบริหารจัดการสำนักงาน (e-office)	เพื่อจัดการและปรับปรุงการทำงานของสำนักงานให้มีประสิทธิภาพมากขึ้น โดยทั่วไปแล้ว ระบบสารบรรณ ระบบพัสดุ ระบบบุคคล ระบบจองห้องประชุม ระบบจองรถ
ระบบบริหารจัดการบุคคล (Humansoft)	เพื่อจัดการและปรับปรุงการทำงานของบุคลากรภายในสถาบันให้มีประสิทธิภาพมากขึ้น โดยทั่วไปแล้ว ระบบลา ระบบเข้างาน-ออกงาน ระบบสวัสดิการ

๙.๒ การพิจารณาผลกระทบจากการหยุดชะงักของกระบวนการหรือบริการที่สำคัญ

เมื่อทำการรวบรวมข้อมูลตามในตารางข้างต้นแล้ว สถาบันพิจารณาผลกระทบ โดยพิจารณาจากข้อมูลในตารางผลกระทบเมื่อกระบวนการทางธุรกิจหรือบริการที่สำคัญต่อภารกิจของสถาบันหยุดชะงัก ดังตารางต่อไปนี้

ตารางที่ ๒๔ ระดับการพิจารณาผลกระทบ

วัตถุประสงค์ด้านความมั่นคงปลอดภัยไซเบอร์ (Security Objective)	ผลกระทบที่อาจเกิดขึ้น (potential impact)		
	ต่ำ	กลาง	สูง
ด้านการรักษาความลับ (Confidentiality)	การเปิดเผยข้อมูลโดยไม่ได้รับอนุญาตอาจส่งผลกระทบน้อยหรืออย่างจำกัด (Limited) และเกิดผลประโยชน์สถาบันสำคัญน้อย (Less Important or Secondary National Interests)	การเปิดเผยข้อมูลโดยไม่ได้รับอนุญาต อาจส่งผลกระทบอย่างร้ายแรง (Serious) และเกิดผลประโยชน์สถาบันที่สำคัญ (Important National Interests)	การเปิดเผยข้อมูลโดยไม่ได้รับอนุญาตอาจส่งผลกระทบอย่างร้ายแรงมา (Severe or Catastrophic) และเกิดผลประโยชน์สถาบันสำคัญยิ่ง(Extremely Important National Interests)
	มีผลกระทบต่อข้อมูลที่ลับ (ข้อมูลข่าวสารลับซึ่งหากเปิดเผยทั้งหมดหรือเพียงบางส่วนจะก่อให้เกิดความเสียหายแก่ประโยชน์แห่งรัฐ)	มีผลกระทบต่อข้อมูลที่ลับมาก (ข้อมูลข่าวสารลับซึ่งหากเปิดเผยทั้งหมดหรือเพียงบางส่วนจะก่อให้เกิดความเสียหายแก่ประโยชน์แห่งรัฐอย่างร้ายแรง)	มีผลกระทบต่อข้อมูลที่ลับที่สุด (ข้อมูลข่าวสารลับซึ่งหากเปิดเผยทั้งหมดหรือเพียงบางส่วนจะก่อให้เกิดความเสียหายแก่ประโยชน์แห่งรัฐอย่างร้ายแรงที่สุด)
ด้านการรักษาความถูกต้องครบถ้วน (Integrity)	การแก้ไขหรือทำลายข้อมูลโดยไม่ได้รับอนุญาตอาจส่งผลกระทบน้อยหรืออย่างจำกัด (Limited) และเกิดผลประโยชน์สถาบันสำคัญน้อย (Less Important or Secondary National Interests)	การแก้ไขหรือทำลายข้อมูลโดยไม่ได้รับอนุญาตอาจส่งผลกระทบอย่างร้ายแรง (Serious) และเกิดผลประโยชน์สถาบันที่สำคัญ (Important National Interests)	การแก้ไขหรือทำลายข้อมูลโดยไม่ได้รับอนุญาตอาจส่งผลกระทบอย่างร้ายแรงมาก (Severe or Catastrophic) และเกิดผลประโยชน์สถาบันสำคัญยิ่ง (Extremely Important National Interests)

วัตถุประสงค์ด้านความมั่นคงปลอดภัยไซเบอร์ (Security Objective)	ผลกระทบที่อาจเกิดขึ้น (potential impact)		
	ต่ำ	กลาง	สูง
ด้านการรักษาสภาพพร้อมใช้งาน (Availability)	การหยุดชะงักของการเข้าถึงหรือการใช้ข้อมูลข่าวสารหรือระบบสารสนเทศอาจส่งผลกระทบน้อยหรืออย่างจำกัด (Limited) และเกิดผลประโยชน์สถาบันสำคัญน้อย (Less Important or Secondary National Interests)	การหยุดชะงักของการเข้าถึงหรือการใช้ข้อมูลข่าวสารหรือระบบสารสนเทศอาจส่งผลกระทบอย่างร้ายแรง (Serious) และเกิดผลประโยชน์สถาบันที่สำคัญ (Important National Interests)	การหยุดชะงักของการเข้าถึงหรือการใช้ข้อมูลข่าวสารหรือระบบสารสนเทศอาจส่งผลกระทบอย่างร้ายแรงมาก (Severe or Catastrophic) และเกิดผลประโยชน์สถาบันสำคัญยิ่ง (Extremely Important National Interests)

ตารางที่ ๒๕ การประเมินผลกระทบด้านต่าง ๆ และระดับผลกระทบต่อบริการที่สำคัญ

กระบวนการทางธุรกิจ	ผลกระทบด้านต่าง ๆ			ระดับผลกระทบ		
	การดำเนินงาน	การให้บริการ	ชื่อเสียง	ด้านการรักษาความลับ	ด้านการรักษาความถูกต้องครบถ้วน	ด้านการรักษาสภาพพร้อมใช้งาน
๑. ระบบเว็บไซต์สถาบัน โดเมนเนม itd.or.th	กระทบผู้ใช้งานระบบ	กระทบผู้ใช้งานระบบเกิดความขัดข้อง	อาจจะถูกกระทบความน่าเชื่อถือขององค์กร	กลาง	กลาง	ต่ำ
๒. ระบบเว็บไซต์สถาบัน โดเมนเนม BCGconnex.com	กระทบผู้ใช้งานระบบ	กระทบผู้ใช้งานระบบเกิดความขัดข้อง	อาจจะถูกกระทบความน่าเชื่อถือขององค์กร	กลาง	กลาง	ต่ำ

กระบวนการทางธุรกิจ	ผลกระทบด้านต่าง ๆ			ระดับผลกระทบ		
	การดำเนินงาน	การให้บริการ	ชื่อเสียง	ด้านการรักษาความลับ	ด้านการรักษาความถูกต้องครบถ้วน	ด้านการรักษาสภาพพร้อมใช้งาน
๓.ระบบสารสนเทศในการบริหารจัดการองค์กร ด้านงบประมาณ การเงิน บัญชี และวัสดุ (e-Budget)	กระทบผู้ใช้งานระบบ	กระทบผู้ใช้งานระบบเกิดความขัดข้อง	อาจจะถูกกระทบความน่าเชื่อถือขององค์กร	สูง	กลาง	ต่ำ
๔. ระบบ Prompt Pass	กระทบผู้ใช้งานระบบ	กระทบผู้ใช้งานระบบเกิดความขัดข้อง	อาจจะถูกกระทบความน่าเชื่อถือขององค์กร	กลาง	กลาง	ต่ำ
๕. ระบบคลาวด์เว็บ Prompt Pass	กระทบผู้ใช้งานระบบ	กระทบผู้ใช้งานระบบเกิดความขัดข้อง	อาจจะถูกกระทบความน่าเชื่อถือขององค์กร	กลาง	กลาง	ต่ำ
๖. ระบบบริหารจัดการสำนักงาน	กระทบผู้ใช้งานระบบ	กระทบผู้ใช้งานระบบเกิดความขัดข้อง	อาจจะถูกกระทบความน่าเชื่อถือขององค์กร	กลาง	กลาง	ต่ำ

ตารางที่ ๒๖ คุณลักษณะความมั่นคงปลอดภัยไซเบอร์ของระบบสารสนเทศที่ใช้สนับสนุนกระบวนการชำระหนี้

กระบวนการ	ระบบสารสนเทศ	ประเภทข้อมูลที่อยู่ในระบบ	ระดับผลกระทบที่อาจเกิดขึ้น		
			ด้านการรักษาความลับ	ด้านการรักษาความถูกต้องครบถ้วน	ด้านการรักษาสภาพพร้อมใช้งาน
ระบบเว็บไซต์สถาบัน โดเมนเนม itd.or.th	เครื่องแม่ข่ายเว็บไซต์	ข้อมูลสถาบัน	กลาง	ต่ำ	ต่ำ
		ข้อมูลการวิจัยสถาบัน	กลาง	กลาง	ต่ำ
		สรุประดับผลกระทบ	กลาง	กลาง	ต่ำ
ระบบเว็บไซต์สถาบัน โดเมนเนม BCGconnex.com	ระบบคลาวด์	ข้อมูลผู้ประกอบการ	กลาง	ต่ำ	ต่ำ
		ข้อมูลสินค้าผู้ประกอบการ	กลาง	กลาง	ต่ำ
		สรุประดับผลกระทบ	กลาง	กลาง	ต่ำ
ระบบสารสนเทศในการบริหารจัดการองค์กร ด้านงบประมาณ การเงิน บัญชี และวัสดุ (e-Budget)	ระบบคลาวด์	ข้อมูลการเงินสถาบัน	กลาง	ต่ำ	ต่ำ
		ข้อมูลการใช้งบประมาณ	สูง	กลาง	ต่ำ
		สรุประดับผลกระทบ	กลาง	กลาง	ต่ำ
ระบบ Prompt Pass	ระบบคลาวด์	ข้อมูลผู้เชี่ยวชาญ	กลาง	ต่ำ	ต่ำ
		ข้อมูลการปรึกษาผู้เชี่ยวชาญ	กลาง	กลาง	ต่ำ
		สรุประดับผลกระทบ	กลาง	กลาง	ต่ำ
ระบบคลาวด์เว็บ Prompt Pass	ระบบคลาวด์	ข้อมูลผู้เชี่ยวชาญ	กลาง	ต่ำ	ต่ำ
		ข้อมูลการปรึกษาผู้เชี่ยวชาญ	กลาง	กลาง	ต่ำ

กระบวนการ	ระบบสารสนเทศ	ประเภทข้อมูลที่อยู่ในระบบ	ระดับผลกระทบที่อาจเกิดขึ้น		
			ด้านการรักษาความลับ	ด้านการรักษาความถูกต้องครบถ้วน	ด้านการรักษาสภาพพร้อมใช้งาน
		สรุประดับผลกระทบ	กลาง	กลาง	ต่ำ
ระบบบริหารจัดการสำนักงาน	ระบบคลาวด์ Saas	ข้อมูลเจ้าหน้าที่	กลาง	ต่ำ	ต่ำ
		ข้อมูลการสำนักงาน	กลาง	กลาง	ต่ำ
		สรุประดับผลกระทบ	กลาง	กลาง	ต่ำ

๙.๓ การพิจารณาผลกระทบจากการหยุดชะงักของกระบวนการหรือบริการที่สำคัญ

ตารางที่ ๒๗ สถาบันระบุระยะเวลา MTD RTO และ RPO ดังตารางต่อไปนี้

กระบวนการทางธุรกิจ	MTD	RTO	RPO
ระบบเว็บไซต์สถาบันโดเมนเนม itd.or.th	๔๘ ชั่วโมง	๒๔ ชั่วโมง	๒๔ ชั่วโมง
ระบบเว็บไซต์สถาบัน BCGconnex.com	๔๘ ชั่วโมง	๒๔ ชั่วโมง	๒๔ ชั่วโมง
ระบบสารสนเทศในการบริหารจัดการองค์กรด้านงบประมาณ การเงิน บัญชี และวัสดุ (e-Budget)	๗๒ ชั่วโมง	๒๔ ชั่วโมง	๒๔ ชั่วโมง
ระบบ Prompt Pass	๗๒ ชั่วโมง	๒๔ ชั่วโมง	๒๔ ชั่วโมง
ระบบคลาวด์เว็บ Prompt Pass	๗๒ ชั่วโมง	๒๔ ชั่วโมง	๒๔ ชั่วโมง

๙.๔ ระบุทรัพยากรที่ต้องใช้ในการดำเนินการ

ตารางที่ ๒๘ ระบุทรัพยากรที่เกี่ยวข้องกับกระบวนการทางธุรกิจที่ต้องใช้ในการดำเนินการ

ทรัพยากรของระบบ/อุปกรณ์ต่าง ๆ	แพลตฟอร์ม/ระบบปฏิบัติการ/เวอร์ชัน	คำอธิบาย
ระบบคลาวด์เว็บ itd.or.th	CentOS ๗	เป็นระบบคลาวด์ที่ให้บริการเว็บ

ทรัพยากรของระบบ/อุปกรณ์ต่าง ๆ	แพลตฟอร์ม/ ระบบปฏิบัติการ/เวอร์ชัน	คำอธิบาย
ระบบคลาวด์เว็บ BCGconnex	Windows Server ๒๐๑๙ Standard ๖๔-bit (๑๐.๐, Build ๑๗๗๖๓)	เป็นระบบคลาวด์ที่ให้บริการเว็บ
ระบบสารสนเทศในการบริหารจัดการองค์กร ด้านงบประมาณ การเงิน บัญชี และวัสดุ (e-Budget)	ubuntu	เป็นระบบจัดการงบประมาณภายในสถาบัน
ระบบ Prompt Pass	ubuntu	เป็นระบบจัดการฐานข้อมูลผู้เชี่ยวชาญและให้คำปรึกษาผู้ประกอบการ
ระบบคลาวด์เว็บ Prompt Pass	ubuntu	เป็นเว็บไซต์ฐานข้อมูลผู้เชี่ยวชาญและให้คำปรึกษาผู้ประกอบการ
ระบบบริหารจัดการสำนักงาน	SaaS	เป็นระบบคลาวด์ที่ให้บริการจัดการสำนักงานผ่านทาง สพร.

๙.๕ ระบุระยะเวลาเป้าหมายในการกู้คืน

ตารางที่ ๒๙ การระบุระยะเวลาเป้าหมายในการกู้คืนทรัพยากรตามรายการทรัพยากรของระบบ/อุปกรณ์ต่าง ๆ จากตารางที่ ๒๘ (ข้อที่ ๙.๔)

ระดับความสำคัญ	แพลตฟอร์ม/ ระบบปฏิบัติการ/เวอร์ชัน	ระยะเวลาเป้าหมายในการกู้คืน (RTO)
เครื่องแม่ข่ายเว็บ itd.or.th	CentOs๗	๒๔ ชั่วโมง ในการนำกลับมาใช้งานได้ใหม่ และ/หรือ นำเครื่องใหม่มาแทนที่
เครื่องแม่ข่ายเว็บ BCGconnex	Windows Server ๒๐๑๙ Standard ๖๔-bit (๑๐.๐, Build ๑๗๗๖๓)	๒๔ ชั่วโมง ในการนำกลับมาใช้งานได้ใหม่ และ/หรือ นำเครื่องใหม่มาแทนที่
ระบบคลาวด์ Prompt Pass	ubuntu	๗๒ ชั่วโมง ในการนำกลับมาใช้งานได้ใหม่ และ/หรือ นำเครื่องใหม่มาแทนที่
ระบบคลาวด์เว็บ Prompt Pass	ubuntu	๗๒ ชั่วโมง ในการนำกลับมาใช้งานได้ใหม่ และ/หรือ นำเครื่องใหม่มาแทนที่
ระบบสารสนเทศในการบริหารจัดการองค์กร ด้านงบประมาณ การเงิน บัญชี และวัสดุ (e-Budget)	ubuntu	๗๒ ชั่วโมง ในการนำกลับมาใช้งานได้ใหม่ และ/หรือ นำเครื่องใหม่มาแทนที่