BUSINESS PLAN

แผนจัดการความต่อเนื่องทางธุรกิจ

2569

ศูนย์คุณธรรม
(องค์การมหาชน)

ศูนย์คุณธรรม (องค์การมหาชน)
กลุ่มงานศูนย์ข้อมูลและเทคโนโลยีสารสนเทศ
เลขที่ 69 อาคารวิทยาลัยการจัดการ มหาวิทยาลัยมหิดล (CMMU) ชั้น 16-17, 21
ถ.วิภาวดีรังสิต แขวงสามเสนใน เขตพญาไท กรุงเทพฯ 10400

แผนจัดการความต่อเนื่องทางธุรกิจ

(Business Continuity Plan - BCP)

ประจำปี 2569

เลขที่เอกสาร	BCP-IT-001	ระดับความลับ	ใช้ภายในหน่วยงาน
วันที่บังคับใช้	1 เมษายน 2569	เวอร์ชัน	1.0

คำนำ

แผนจัดการความต่อเนื่องทางธุรกิจ (Business Continuity Plan: BCP) ฉบับนี้ ได้ทำขึ้นเพื่อเป็นกรอบแนวทางและกระบวนการที่เป็นระบบ (Systematic Framework) สำหรับรองรับสถานการณ์ฉุกเฉินและอุบัติการณ์ที่อาจส่งผลกระทบต่อการดำเนินงานขององค์กร โดยมุ่งเน้นที่การเตรียมความพร้อมในการกู้คืนระบบงานที่สำคัญ บริการโครงสร้างพื้นฐานด้านเทคโนโลยีสารสนเทศ และการรักษาระดับการให้บริการตามมาตรฐานที่กำหนด

เนื้อหาภายในเอกสารครอบคลุมตั้งแต่โครงสร้างทีมบริหารจัดการอุบัติการณ์ การวิเคราะห์ผลกระทบทางธุรกิจ (BIA) กลยุทธ์ความต่อเนื่องทางธุรกิจ ขั้นตอนการปฏิบัติงาน (Incident Response Swimlane) ตลอดจนการทดสอบและบำรุงรักษาแผน เพื่อให้มั่นใจว่าบุคลากรและผู้ที่เกี่ยวข้องสามารถตอบสนองต่อเหตุการณ์ได้อย่างมีประสิทธิภาพ ลดผลกระทบจากการหยุดชะงัก (Minimizing Downtime) และสามารถกู้คืนระบบกลับสู่สภาวะปกติได้ภายในระยะเวลาที่กำหนด

คณะผู้จัดทำ

ประจำปี 2569

สารบัญ

1. วัตถุประสงค์และเป้าหมายเชิงยุทธศาสตร์

1.1 วัตถุประสงค์

การจัดทำแผนจัดการความต่อเนื่องทางธุรกิจฉบับนี้
มีวัตถุประสงค์เพื่อวางรากฐานและสร้างกระบวนการที่เป็นระบบ (Systematic Framework)
ในการตอบสนองต่ออุบัติการณ์ โดยมีรายละเอียดดังนี้:

- เพื่อกำหนดโครงสร้างการรับมือเหตุฉุกเฉินและกลไกการตัดสินใจที่ชัดเจน
  ลดความซับซ้อนและข้อผิดพลาดในการปฏิบัติงานเมื่อเกิดภาวะวิกฤต
- เพื่อสร้างความมั่นใจในความพร้อมใช้ (Availability) ของบริการโครงสร้างพื้นฐาน
  ทั้งในส่วนของเครือข่ายภายใน และระบบความปลอดภัยทางกายภาพที่สำคัญ (CCTV, Access Control,
  ระบบดับเพลิงห้อง Data Center)
- เพื่อบูรณาการการทำงานร่วมกับผู้ให้บริการภายนอก (Outsource Vendor) ที่ดูแลระบบเครือข่าย (MA)
  ให้เป็นไปตามมาตรฐานข้อตกลงระดับการให้บริการ (SLA) อย่างมีประสิทธิภาพ

1.2 เป้าหมายเชิงยุทธศาสตร์

- **การรักษาความต่อเนื่องของบริการคลาวด์:** วางระบบและช่องทางสำรอง (Redundancy)
  เพื่อให้บุคลากรสามารถเข้าถึงระบบงานสำคัญบนคลาวด์ได้อย่างไร้รอยต่อ
  แม้โครงสร้างพื้นฐานหลักจะได้รับผลกระทบ
- **การลดผลกระทบจากการหยุดชะงัก (Minimizing Downtime):**
  บรรลุเป้าหมายระยะเวลาการกู้คืนระบบ (RTO) ตามที่หน่วยงานกำหนด เพื่อไม่ให้กระทบต่อภารกิจหลัก
- **การรักษาความสมบูรณ์ของข้อมูล (Data Integrity):**
  ดำเนินการจัดเก็บและปกป้องข้อมูลผ่านระบบคลาวด์อย่างเคร่งครัด
  เพื่อให้มั่นใจว่าจะไม่มีการสูญหายของข้อมูล (Zero Data Loss)

2. โครงสร้างทีมบริหารจัดการอุบัติการณ์

ประกอบด้วย 3 ภาคส่วนหลัก:

- **ผู้บริหาร (Management):** ผู้มีอำนาจประกาศใช้แผน อนุมัติการตัดสินใจเชิงนโยบาย
  และจัดสรรทรัพยากรฉุกเฉิน

- **ทีมงานไอที (IT Operations):** ผู้ตรวจประเมินสถานการณ์เบื้องต้น ควบคุมการกู้คืนระบบและประสานงานเทคนิค
- **ผู้ให้บริการภายนอก (Vendor):** ผู้เชี่ยวชาญที่ดูแลรับผิดชอบสัญญา MA ระบบ Network ในการเข้าแก้ไขปัญหาโครงสร้างหลักและอุปกรณ์ Hardware

3. การวิเคราะห์ผลกระทบทางธุรกิจ (BIA)

ระบบโครงสร้างพื้นฐาน / บริการ	ระดับความสำคัญ	เป้าหมายเวลากู้คืน (RTO)
ระบบงานหลักบน Cloud และอินเทอร์เน็ต	วิกฤต (Critical)	ภายใน 1 - 2 ชั่วโมง
ระบบควบคุมการเข้า-ออก และ CCTV	สูง (High)	ภายใน 4 ชั่วโมง
ระบบเครือข่ายภายใน (LAN/WIFI) และ AD	ปานกลาง (Medium)	ภายใน 8 ชั่วโมง

4. กลยุทธ์ความต่อเนื่องทางธุรกิจ

หน่วยงานกำหนดกลยุทธ์เชิงรุก โดยมุ่งเน้นการจัดเตรียมระบบเครือข่ายสำรองแบบ Dual WAN และการเชื่อมต่อผ่านโครงข่ายโทรศัพท์เคลื่อนที่ (5G Failover) เป็นหัวใจสำคัญในการเข้าถึงคลาวด์ พร้อมทั้งเตรียมกุญแจฉุกเฉิน (Manual Key) สำหรับระบบ Access Control และการสำรองไฟฟ้า (UPS) ที่ครอบคลุมห้อง Data Center เพื่อซื้อเวลาในการแก้ไขปัญหา

5. ขั้นตอนการปฏิบัติงาน (Incident Response Swimlane)

กระบวนการตอบสนองต่อเหตุฉุกเฉินแบ่งตามบทบาทความรับผิดชอบ (Swimlane) เพื่อให้เห็นเส้นทางการปฏิบัติงานที่ชัดเจนบูรณาการร่วมกัน:

ระยะเวลา / ขั้นตอน	ผู้บริหาร (Management)	ทีมงานไอที (IT Operations)	ผู้ให้บริการภายนอก (Vendor MA)
1. ตรวจพบเหตุ (Detection)	-	มอนิเตอร์พบความผิดปกติของระบบ Network/Cloud หรือได้รับแจ้งเหตุขัดข้อง	ระบบ NMS แจ้งเตือนสถานะอุปกรณ์เครือข่ายหยุดทำงาน
2. ประเมินผล (Assessment)	รับรายงานสถานการณ์ฉุกเฉินเบื้องต้น	วิเคราะห์ความรุนแรง หากคาดว่าระบบล่มเกิน RTO ให้เร่งสรุปข้อมูล	ตรวจสอบ Log และประเมินสาเหตุ (Root Cause) ของ Hardware/Link
3. ประกาศใช้แผน (Activation)	อนุมัติการประกาศใช้แผน BCP และสั่งการสื่อสารองค์กร	แจ้งเตือนบุคลากรให้เตรียมใช้ระบบสำรอง / อนุมัติ Vendor เข้าพื้นที่	จัดเตรียมอะไหล่และทีมวิศวกรเข้าแก้ไขตาม SLA (เช่น ภายใน 4 ชม.)
4. กู้คืนระบบ (Recovery)	ติดตามสถานะการแก้ไขปัญหาอย่างใกล้ชิด	เปิดใช้อินเทอร์เน็ตสำรอง (Failover) และดูแลระบบ Security ภายใน	เปลี่ยนอุปกรณ์ Hardware หรือแก้ไข Configuration ที่ไซต์งาน
5. กลับสู่ปกติ (Restoration)	ประกาศยกเลิกภาวะฉุกเฉิน	ทดสอบระบบร่วมกับ User และปรับกลับสู่สภาวะการทำงานหลัก	ส่งมอบรายงานการแก้ไขปัญหา (Incident Report)

6. การทดสอบและบำรุงรักษาแผน

เพื่อให้แผนมีความทันสมัยและพร้อมใช้งาน หน่วยงานจะต้อง:

- จัดการซ้อมแผนบนโต๊ะ (Tabletop Exercise) จำลองสถานการณ์ทางไซเบอร์หรือระบบล่ม อย่างน้อยปีละ 1 ครั้ง
- ทบทวนข้อมูลการติดต่อ (Call Tree) และสัญญากับ Vendor MA ทุกรอบ 6 เดือน

บรรณานุกรม

- พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562.
- ISO/IEC 22301:2019 Security and resilience — Business continuity management systems.
- NIST Special Publication 800-34 Rev. 1: Contingency Planning Guide.