แผนบริหารความต่อเนื่อง
กรณีระบบเทคโนโลยีสารสนเทศขัดข้อง

(Business Continuity Plan : BCP for IT System Failure)

ศูนย์แพทยศาสตรศึกษาชั้นคลินิก โรงพยาบาลสวรรค์ประชารักษ์

งานเทคโนโลยีสารสนเทศ ปีงบประมาณ 2568

สาระสำคัญของแผน

- ใช้เป็นแนวทางปฏิบัติเมื่อระบบเทคโนโลยีสารสนเทศขัดข้องหรือเกิดเหตุฉุกเฉิน
- กำหนดบทบาทผู้รับผิดชอบ ช่องทางสื่อสาร ลำดับการฟื้นฟูระบบ และแนวทางรายงานผล
- มุ่งให้การเรียนการสอน การสื่อสาร และงานสนับสนุนสำคัญดำเนินต่อได้ตามความเหมาะสม

เอกสารฉบับนี้จัดทำเพื่อใช้ภายในศูนย์แพทยศาสตรศึกษาชั้นคลินิก โรงพยาบาลสวรรค์ประชารักษ์

ข้อมูลควบคุมเอกสาร

รายการ	รายละเอียด
ชื่อเอกสาร	แผนบริหารความต่อเนื่อง กรณีระบบเทคโนโลยีสารสนเทศขัดข้อง (BCP-IT)
หน่วยงานรับผิดชอบ	งานเทคโนโลยีสารสนเทศ ศูนย์แพทยศาสตรศึกษาชั้นคลินิก โรงพยาบาลสวรรค์ประชารักษ์
ปีงบประมาณ	2568
ลักษณะเอกสาร	แนวปฏิบัติเมื่อเกิดเหตุขัดข้องด้านเทคโนโลยีสารสนเทศ
การทบทวน	ให้ทบทวนอย่างน้อยปีละ 1 ครั้ง หรือเมื่อมีการเปลี่ยนแปลงระบบสำคัญ โครงสร้างผู้รับผิดชอบ หรือเกิดเหตุการณ์จริง

ตารางสรุปแผน BCP-IT

ประเด็น	แนวทางที่กำหนด
เหตุการณ์ที่ครอบคลุม	ระบบเครือข่ายขัดข้อง, Server/Storage ขัดข้อง, ฐานข้อมูลหรือระบบสารสนเทศไม่พร้อมใช้งาน, เหตุไซเบอร์, ไฟฟ้าขัดข้อง, ภัยธรรมชาติ และเหตุอื่นที่กระทบต่อการเรียนการสอนหรือการสื่อสาร
ระบบสำคัญ	ระบบเครือข่ายและอินเทอร์เน็ต, ระบบเว็บไซต์และการสื่อสาร, ระบบจัดเก็บข้อมูล, ระบบสนับสนุนการเรียนการสอน, ระบบสำรองข้อมูล และระบบ DC/DR
ช่องทางแจ้งเหตุ	QR Code แจ้งปัญหา IT, Line กลุ่ม, Email ของงาน IT, โทรศัพท์ 056-219870 และการแจ้งโดยตรงต่อเจ้าหน้าที่ IT
เป้าหมายการรับมือ	ตรวจพบและรับแจ้งโดยเร็ว, จัดระดับความรุนแรง, สื่อสารสถานะเป็นระยะ, ฟื้นฟูระบบตามลำดับความสำคัญ และรายงานผลหลังเหตุการณ์
ผู้รับผิดชอบหลัก	หัวหน้างานเทคโนโลยีสารสนเทศ/นักวิชาการคอมพิวเตอร์/นายช่างเทคนิค และผู้บริหารศูนย์ฯ ตามระดับเหตุการณ์

โครงสร้างเอกสารโดยสรุป

ส่วน	หัวข้อสำคัญ
ส่วนที่ 1	วัตถุประสงค์ ขอบเขต สมมติฐาน และคำจำกัดความ
ส่วนที่ 2	ระดับเหตุการณ์ ระบบสำคัญ RTO/RPO ผู้รับผิดชอบ และช่องทางสื่อสาร
ส่วนที่ 3	ขั้นตอนปฏิบัติ แผนรองรับรายสถานการณ์ DC/DR และมาตรการควบคุมความเสี่ยง
ส่วนที่ 4	การทดสอบ ตัวชี้วัด การรายงาน และแบบฟอร์มภาคผนวก

1. วัตถุประสงค์ของแผน

กำหนดให้แผนฉบับนี้เป็นแนวทางปฏิบัติกลางสำหรับการบริหารความต่อเนื่องของระบบเทคโนโลยีสารสนเทศ เมื่อเกิดเหตุขัดข้องหรือเหตุฉุกเฉินที่กระทบต่อภารกิจของศูนย์แพทยศาสตรศึกษาชั้นคลินิก โรงพยาบาลสวรรค์ประชารักษ์

1. กำหนดแนวทางการรับมือเหตุขัดข้องด้านเทคโนโลยีสารสนเทศอย่างเป็นระบบและทันเวลา
2. ลดผลกระทบต่อการเรียนการสอน การประสานงาน การสื่อสาร และงานสนับสนุนที่เกี่ยวข้อง
3. กำหนดบทบาท หน้าที่ ช่องทางสื่อสาร และลำดับการตัดสินใจของผู้เกี่ยวข้องให้ชัดเจน
4. กำหนดแนวทางการฟื้นฟูระบบ การสำรองข้อมูล และการรายงานผลหลังเกิดเหตุ
5. ใช้เป็นหลักฐานประกอบการควบคุมภายใน การบริหารความเสี่ยง และการปรับปรุงระบบ IT อย่างต่อเนื่อง

2. ขอบเขตของแผน

แผนนี้ให้ใช้กับระบบเทคโนโลยีสารสนเทศที่สนับสนุนภารกิจของศูนย์ฯ ทั้งในภาวะปกติและภาวะฉุกเฉิน โดยครอบคลุมรายการต่อไปนี้

กลุ่มระบบ/งาน	ขอบเขตที่ครอบคลุม	ผลกระทบที่ต้องควบคุม
ระบบการเรียนการสอน	ระบบสนับสนุนการสอนออนไลน์ สื่อการเรียนการสอน ฐานข้อมูลการเรียน และระบบที่เกี่ยวข้องกับนักศึกษา	การเรียนการสอนหยุดชะงัก การประกาศข้อมูลล่าช้า หรือเข้าถึงข้อมูลไม่ได้
ระบบเครือข่ายและอินเทอร์เน็ต	Switch, Router, Firewall, Wireless, VLAN, Internet และการเชื่อมต่อระหว่างอาคาร	ไม่สามารถเข้าถึงระบบภายในระบบภายนอก หรือบริการออนไลน์ได้
ระบบจัดเก็บและสำรองข้อมูล	Server, Storage, NAS/SAN, Backup, Snapshot และข้อมูลสำคัญของหน่วยงาน	ข้อมูลสูญหายหรือกู้คืนล่าช้า กระทบต่อความต่อเนื่องของงาน
ระบบสื่อสาร	เว็บไซต์ศูนย์ฯ, Email, Line กลุ่ม, โทรศัพท์ และช่องทางประกาศข่าวสาร	ผู้ใช้ไม่ได้รับข้อมูลสถานะระบบหรือแนวทางปฏิบัติที่ถูกต้อง
ความมั่นคงปลอดภัยไซเบอร์	Firewall, Antivirus, Access Control, Log, Monitoring และการตอบสนองต่อเหตุไซเบอร์	ข้อมูลรั่วไหล ระบบติดมัลแวร์ หรือถูกโจมตีจนให้บริการไม่ได้

3. สมมติฐานในการจัดทำแผน

ประเด็นสมมติฐาน	แนวปฏิบัติที่กำหนด
ความเสี่ยงที่อาจเกิดขึ้น	ให้ถือว่าเหตุขัดข้องด้าน IT สามารถเกิดได้จากฮาร์ดแวร์ ซอฟต์แวร์ เครือข่าย ไฟฟ้า ภัยธรรมชาติ ความผิดพลาดของผู้ใช้ หรือภัยคุกคามทางไซเบอร์
ความสำคัญของระบบ IT	ให้จัดระบบ IT เป็นโครงสร้างพื้นฐานสำคัญที่สนับสนุนการเรียนการสอน การสื่อสาร และการจัดเก็บข้อมูลของศูนย์ฯ
ทรัพยากรและบุคลากร	ให้ทีม IT ดำเนินการตามลำดับความสำคัญของเหตุการณ์ และประสานผู้บริหาร/หน่วยงานสนับสนุนเมื่อเกินขีดความสามารถ

ประเด็นสมมติฐาน	แนวปฏิบัติที่กำหนด
การสนับสนุนจากผู้บริหาร	ให้ผู้บริหารพิจารณาอนุมัติทรัพยากร การสื่อสาร และมาตรการรองรับภาวะฉุกเฉินตามระดับเหตุการณ์
การกู้คืนระบบ	ให้ระบบสำคัญมีแนวทางสำรองข้อมูลและแผนฟื้นฟู โดยกำหนดเป้าหมาย RTO/RPO ให้สอดคล้องกับความสำคัญของระบบ
การทบทวนแผน	ให้ทบทวนแผนอย่างน้อยปีละ 1 ครั้ง และภายหลังเกิดเหตุการณ์จริงหรือการทดสอบแผน

4. คำจำกัดความที่ใช้ในแผน

คำ	ความหมายในการปฏิบัติ
BCP-IT	แผนบริหารความต่อเนื่องกรณีระบบเทคโนโลยีสารสนเทศขัดข้อง
Incident	เหตุขัดข้องหรือเหตุผิดปกติที่กระทบต่อระบบ IT หรือการให้บริการ
RTO	ระยะเวลาสูงสุดที่ยอมรับได้ในการฟื้นฟูระบบให้กลับมาใช้งานได้
RPO	ช่วงเวลาข้อมูลย้อนหลังสูงสุดที่ยอมรับได้หากต้องกู้คืนข้อมูล
DC	ศูนย์ข้อมูลหลักที่ใช้ให้บริการระบบสารสนเทศของศูนย์ฯ
DR	ระบบหรือสถานที่สำรองเพื่อใช้กู้คืนบริการเมื่อระบบหลักไม่พร้อมใช้งาน
Priority	ระดับความเร่งด่วนของเหตุการณ์ เพื่อกำหนดลำดับการแก้ไขและการสื่อสาร

5. ระดับเหตุการณ์และการจัดลำดับความเร่งด่วน

เมื่อได้รับแจ้งเหตุ ให้ทีม IT ประเมินผลกระทบ จำนวนผู้ได้รับผลกระทบ ระยะเวลาที่เกิดเหตุ และความสำคัญของระบบ เพื่อกำหนดระดับความเร่งด่วน ดังนี้

ระดับ	ลักษณะเหตุการณ์	ระยะเวลาตอบสนองเบื้องต้น	การสื่อสาร/รายงาน
Critical	ระบบสำคัญหยุดให้บริการเป็นวงกว้าง กระทบการเรียนการสอน/การสื่อสารหลัก หรือมีความเสี่ยงด้านข้อมูลรั่วไหล	ทันที หรือไม่เกิน 15 นาที	รายงานผู้บริหารทันที และแจ้งผู้ใช้เป็นระยะ
High	ระบบสำคัญบางส่วนขัดข้อง ผู้ใช้หลายกลุ่มได้รับผลกระทบ แต่ยังมีช่องทางสำรอง	ไม่เกิน 30 นาที	แจ้งหัวหน้างานและผู้ใช้ที่ได้รับผลกระทบ
Medium	ระบบงานทั่วไปขัดข้อง กระทบเฉพาะบางหน่วย/บางอุปกรณ์	ภายใน 1 วันทำการ	บันทึกในระบบรับแจ้งและแจ้งผลผู้ใช้
Low	ปัญหาเฉพาะราย ไม่กระทบระบบหลัก หรือเป็นคำขอสนับสนุนทั่วไป	ตามลำดับงานบริการ	บันทึกและดำเนินการตามรอบงานปกติ

6. ระบบสำคัญและเป้าหมายการกู้คืน

ระบบ/บริการ	ลำดับความสำคัญ	เป้าหมาย RTO	เป้าหมาย RPO	แนวทางสำรอง
เครือข่ายหลักและอินเทอร์เน็ต	1	ไม่เกิน 4 ชั่วโมง	ไม่เกี่ยวกับข้อมูล	ใช้เส้นทางสำรอง/อุปกรณ์สำรอง/ประสานผู้ให้บริการ
ระบบ Server และ Storage หลัก	1	ไม่เกิน 4 ชั่วโมง	ไม่เกิน 1 ชั่วโมงตามความพร้อมของระบบสำรอง	กู้คืนจาก Snapshot/Backup และ DR ตามลำดับ
ระบบเว็บไซต์และประกาศข่าวสาร	2	ไม่เกิน 8 ชั่วโมง	ไม่เกิน 24 ชั่วโมง	ใช้ช่องทาง Line/Email/ประกาศสำรองระหว่างกู้คืน
ระบบสนับสนุนการเรียนการสอน	2	ไม่เกิน 1 วันทำการ	ไม่เกิน 24 ชั่วโมง	ใช้เอกสาร/ไฟล์สำรอง/ช่องทางสื่อสารสำรอง
เครื่องคอมพิวเตอร์และอุปกรณ์ผู้ใช้	3	ตามลำดับ Priority	ขึ้นกับการจัดเก็บข้อมูล	ใช้เครื่องสำรอง/ซ่อมเปลี่ยนอุปกรณ์/ให้บริการเฉพาะจุด

7. โครงสร้างผู้รับผิดชอบ

ตำแหน่ง/บทบาท	หน้าที่หลักเมื่อเกิดเหตุ	การประสานงาน
ผู้อำนวยการศูนย์แพทยศาสตรศึกษาชั้นคลินิก	พิจารณาสั่งการ อนุมัติทรัพยากร และกำกับการสื่อสารในเหตุการณ์สำคัญ	ประสานผู้บริหารโรงพยาบาลและหน่วยงานที่เกี่ยวข้อง
หัวหน้างานเทคโนโลยีสารสนเทศ	ควบคุมการดำเนินงานตามแผน ประเมินระดับเหตุการณ์ และกำหนดลำดับการฟื้นฟู	รายงานผู้บริหารและประสานทีม IT/หน่วยงานสนับสนุน
นักวิชาการคอมพิวเตอร์	รับผิดชอบระบบแม่ข่าย เครือข่าย ฐานข้อมูล ระบบสำรอง และการกู้คืนบริการ IT	ประสานผู้ใช้ ผู้ให้บริการ และหน่วยงาน IT ที่เกี่ยวข้อง
นายช่างเทคนิค	สนับสนุนการตรวจสอบอุปกรณ์ ซ่อมบำรุง เครือข่ายปลายทาง และติดตั้งอุปกรณ์ทดแทน	ประสานพัสดุ ช่างภายนอก และผู้ใช้บริการ
เจ้าหน้าที่ศูนย์ฯ/ผู้ใช้ระบบ	แจ้งเหตุผ่านช่องทางที่กำหนด ให้ข้อมูลอาการ และปฏิบัติตามประกาศสถานะระบบ	ประสานกับงาน IT และหัวหน้างานของตน

8. ช่องทางแจ้งเหตุและการสื่อสารภาวะวิกฤติ

ช่องทาง	การใช้งาน	ผู้รับผิดชอบ	หมายเหตุ
QR Code แจ้งปัญหา IT	ใช้รับแจ้งปัญหาจากผู้ใช้ทั่วไป พร้อมระบุเวลา สถานที่ อาการ และผู้แจ้ง	ทีม IT	ใช้เป็นหลักฐานการรับแจ้งและติดตามผล
Line กลุ่ม/Line งาน	ใช้แจ้งเหตุเร่งด่วน แจ้งสถานะ และประสานงานระหว่างทีม	ทีม IT/ผู้เกี่ยวข้อง	ให้บันทึกข้อมูลสำคัญลงแบบฟอร์มภายหลัง
Email ของงาน IT	ใช้รับเรื่อง รายงานผล และส่งข้อมูลประกอบเหตุการณ์	ทีม IT	เหมาะสำหรับเอกสารแนบและรายงาน
โทรศัพท์ 056-219870	ใช้แจ้งเหตุเร่งด่วนหรือกรณีระบบออนไลน์ไม่พร้อมใช้งาน	เจ้าหน้าที่เวร/ทีม IT	ให้บันทึกเวลาและรายละเอียดผู้แจ้ง
ประกาศหน้าเว็บไซต์/ช่องทางสำรอง	ใช้แจ้งผู้ใช้วงกว้างเมื่อระบบสำคัญขัดข้อง	ทีมสื่อสาร/ทีม IT	ให้ใช้ข้อความกลางที่ผ่านการตรวจสอบ

หลักเกณฑ์การสื่อสาร

- เหตุระดับ Critical ให้รายงานผู้บริหารโดยทันที และแจ้งสถานะให้ผู้ใช้ทราบเป็นระยะ
- ข้อความแจ้งเตือนต้องระบุระบบที่ได้รับผลกระทบ ระยะเวลาคาดการณ์ แนวทางสำรอง และช่องทางติดต่อ
- หลังแก้ไขแล้ว ให้แจ้งปิดเหตุ พร้อมสรุปสาเหตุเบื้องต้นและข้อควรปฏิบัติของผู้ใช้

9. ขั้นตอนปฏิบัติเมื่อเกิดเหตุขัดข้อง

ลำดับ	ขั้นตอน	แนวทางปฏิบัติ	ผู้รับผิดชอบ	กรอบเวลา
1	รับแจ้งเหตุ	รับแจ้งผ่าน QR Code, Line, Email, โทรศัพท์ หรือแจ้งโดยตรง และบันทึกเวลา สถานที่ อาการ และผู้แจ้ง	ทีม IT/เจ้าหน้าที่รับเรื่อง	ทันที
2	ตรวจสอบเบื้องต้น	ตรวจสอบว่ากระทบระบบใด จำนวนผู้ได้รับผลกระทบ ระดับความเร่งด่วน และมีช่องทางสำรองหรือไม่	นักวิชาการคอมพิวเตอร์/นายช่างเทคนิค	ภายใน 30 นาที
3	ควบคุมสถานการณ์	แยกระบบที่มีปัญหา จำกัดการกระจายของเหตุ และป้องกันผลกระทบต่อระบบอื่น	ทีม IT	ตามระดับเหตุ
4	วินิจฉัยและแก้ไข	ตรวจสอบ Log, Network, Server, Storage, Database, Power, UPS และอุปกรณ์ที่เกี่ยวข้อง แล้วดำเนินการแก้ไข	ทีม IT/ผู้ให้บริการ	ภายใน 1 วัน หรือเร็วที่สุดตามเหตุ
5	ใช้แผนสำรอง	หากไม่สามารถแก้ไขได้ทันเวลา ให้เปิดใช้ช่องทางสำรอง ระบบสำรอง หรือวิธีปฏิบัติงานชั่วคราว	หัวหน้างาน IT/ผู้บริหาร	ตาม RTO
6	ทดสอบและคืนระบบ	ทดสอบการทำงาน ความเสถียร และความถูกต้องของข้อมูลก่อนคืนบริการให้ผู้ใช้	ทีม IT/ผู้ใช้งานหลัก	ก่อนประกาศใช้งาน
7	รายงานและปิดเหตุ	จัดทำสรุปเหตุการณ์ สาเหตุ ผลกระทบ วิธีแก้ไข ระยะเวลา และข้อเสนอป้องกันเหตุซ้ำ	ทีม IT	ภายใน 7 วันทำการ

10. ขั้นตอนการตัดสินใจเปิดใช้แผน BCP-IT

เงื่อนไข	การดำเนินการ	ผู้มีอำนาจ/ผู้ประสาน
ระบบสำคัญหยุดให้บริการเกินระยะเวลาที่กำหนด หรือมีแนวโน้มเกิน RTO	ให้หัวหน้างาน IT เสนอเปิดใช้แผน BCP-IT และกำหนดลำดับฟื้นฟูระบบ	หัวหน้างาน IT / ผู้อำนวยการศูนย์ฯ
เกิดเหตุไซเบอร์หรือสงสัยข้อมูลรั่วไหล	ให้แยกระบบที่เกี่ยวข้อง เก็บหลักฐาน Log และประสานหน่วยงานด้านความมั่นคงปลอดภัยสารสนเทศ	ทีม IT / ผู้บริหาร
ระบบหลักไม่สามารถฟื้นฟูได้ตามเป้าหมาย	ให้พิจารณาใช้ระบบสำรอง DR หรือวิธีปฏิบัติงานทดแทนตามความจำเป็น	ผู้บริหาร / ทีม IT
เหตุการณ์มีผลกระทบต่อผู้ใช้วงกว้าง	ให้สื่อสารสถานะต่อผู้ใช้ผ่านช่องทางที่กำหนด และปรับปรุงข้อมูลเป็นระยะ	ทีม IT / ทีมสื่อสาร

11. แผนรองรับรายสถานการณ์

11.1 กรณีระบบเครือข่ายหรืออินเทอร์เน็ตขัดข้อง

ขั้นตอน	แนวปฏิบัติ
ตรวจสอบ	ให้ตรวจสอบอุปกรณ์เครือข่ายหลัก Switch, Firewall, Router, Wireless Controller, Link Internet และสถานะไฟฟ้า/UPS
จำกัดผลกระทบ	ให้แยกวงจรหรืออุปกรณ์ที่ผิดปกติ และป้องกันไม่ให้กระทบระบบอื่น
ใช้ช่องทางสำรอง	ให้พิจารณาใช้ Link สำรอง อุปกรณ์สำรอง หรือช่องทางสื่อสารสำรองตามความเหมาะสม
ประสานงาน	ให้ประสานผู้ให้บริการอินเทอร์เน็ตหรือผู้ดูแลอุปกรณ์ เมื่อปัญหาเกินขีดความสามารถของทีม IT
รายงานผล	ให้แจ้งสถานะต่อผู้ใช้และผู้บริหาร พร้อมบันทึกเวลาเริ่มเหตุ เวลาแก้ไข และสาเหตุ

11.2 กรณี Server, Storage หรือฐานข้อมูลขัดข้อง

ขั้นตอน	แนวปฏิบัติ
ตรวจสอบ	ให้ตรวจสอบสถานะ Server, Storage, Virtual Machine, Database, Disk, CPU, Memory และ Log ที่เกี่ยวข้อง
ป้องกันข้อมูลเสียหาย	ห้ามดำเนินการที่อาจทำให้ข้อมูลเสียหายเพิ่มเติม หากยังไม่ทราบสาเหตุ ให้สำรองสถานะและเก็บ Log ก่อนแก้ไข
กู้คืนบริการ	ให้ดำเนินการ Restart เฉพาะส่วนที่จำเป็น ย้ายบริการ กู้คืนจาก Backup/Snapshot หรือใช้ระบบ DR ตามระดับความรุนแรง
ตรวจสอบข้อมูล	ให้ทดสอบความถูกต้องของข้อมูลและการเชื่อมต่อกับระบบอื่นก่อนประกาศคืนบริการ

ขั้นตอน	แนวปฏิบัติ
สรุปผล	ให้จัดทำรายงานผลการกู้คืน ระบุ RTO/RPO ที่เกิดขึ้นจริง และข้อเสนอปรับปรุง

11.3 กรณีถูกโจมตีทางไซเบอร์หรือสงสัยข้อมูลรั่วไหล

ขั้นตอน	แนวปฏิบัติ
หยุดการแพร่กระจาย	ให้ตัดการเชื่อมต่อเครื่องหรือระบบที่สงสัยติดมัลแวร์/ถูกโจมตีออกจากเครือข่ายทันที โดยไม่ลบหลักฐาน
เก็บหลักฐาน	ให้เก็บ Log, เวลาเกิดเหตุ, IP, บัญชีผู้ใช้ที่เกี่ยวข้อง และภาพหน้าจอหรือไฟล์หลักฐานตามความเหมาะสม
ประเมินผลกระทบ	ให้ประเมินว่ากระทบข้อมูลส่วนบุคคล ระบบการเรียนการสอน หรือระบบสำคัญอื่นหรือไม่
แจ้งผู้เกี่ยวข้อง	ให้รายงานผู้บริหารและประสานหน่วยงานด้านความมั่นคงปลอดภัยสารสนเทศของโรงพยาบาลตามความเหมาะสม
ฟื้นฟูและป้องกันซ้ำ	ให้กู้คืนจากแหล่งข้อมูลที่ปลอดภัย เปลี่ยนรหัสผ่าน ตรวจสอบสิทธิ์ และปรับปรุงมาตรการป้องกัน

11.4 กรณีไฟฟ้าขัดข้องหรือภัยธรรมชาติ

ขั้นตอน	แนวปฏิบัติ
ประเมินความปลอดภัย	ให้ตรวจสอบความปลอดภัยของบุคลากร ห้องระบบ อุปกรณ์ไฟฟ้า UPS และระบบปรับอากาศก่อนดำเนินการใด ๆ
ป้องกันระบบเสียหาย	ให้ปิดระบบตามลำดับที่กำหนดหากไฟฟ้าสำรองไม่เพียงพอ หรือมีความเสี่ยงต่ออุปกรณ์
ใช้ระบบสำรอง	ให้ใช้ช่องทางสื่อสารสำรองและระบบสำรองตามความพร้อมของอุปกรณ์และความปลอดภัยของสถานที่
กู้คืนหลังเหตุ	ให้ตรวจสอบไฟฟ้า อุณหภูมิ ความชื้น อุปกรณ์เครือข่าย Server และ Storage ก่อนเปิดระบบ
รายงาน	ให้รายงานความเสียหาย รายการอุปกรณ์ที่ได้รับผลกระทบ และความจำเป็นในการจัดซื้อ/ซ่อมแซม

12. การบริหารจัดการระบบศูนย์ข้อมูล (DC) และระบบสำรองฉุกเฉิน (DR)

ให้ใช้แนวทางต่อไปนี้เป็นหลักในการดูแลศูนย์ข้อมูลหลักและระบบสำรองฉุกเฉิน
เพื่อให้ระบบเทคโนโลยีสารสนเทศสามารถสนับสนุนภารกิจได้ต่อเนื่องแม้เกิดเหตุขัดข้องรุนแรง

หัวข้อ	แนวปฏิบัติที่กำหนด
ระบบศูนย์ข้อมูลหลัก (Primary DC)	ให้ตั้งอยู่ในพื้นที่ที่มีระบบไฟฟ้าสำรอง การควบคุมอุณหภูมิ และการจำกัดการเข้าถึงที่เหมาะสม พร้อมตรวจสอบความพร้อมอย่างสม่ำเสมอ
ระบบสำรอง DR	ให้จัดเตรียมหรือพัฒนาระบบ Server/SAN/Storage สำรองตามแผน เพื่อรองรับการย้ายบริการหรือกู้คืนระบบสำคัญเมื่อระบบหลักไม่พร้อมใช้งาน
การสำรองข้อมูล	ให้สำรองข้อมูลตามรอบที่กำหนด โดยอย่างน้อยต้องมี Snapshot รายเดือน และพิจารณาเพิ่มรอบสำรองสำหรับระบบที่มีความสำคัญสูง
การทดสอบกู้คืน	ให้ทดสอบการกู้คืนข้อมูลและระบบอย่างน้อยปีละ 1 ครั้ง หรือหลังการเปลี่ยนแปลงระบบสำคัญ
เป้าหมายการกู้คืน	ให้ตั้งเป้า RTO ไม่เกิน 4 ชั่วโมงสำหรับระบบสำคัญ และ RPO ไม่เกิน 1 ชั่วโมงเมื่อระบบสำรองรองรับได้ ทั้งนี้ให้ปรับตามความพร้อมจริงของระบบ

13. มาตรการควบคุมและลดความเสี่ยง

ความเสี่ยง	มาตรการควบคุม	หลักฐาน/การติดตาม
ระบบขัดข้องจากอุปกรณ์หรือซอฟต์แวร์	ให้บำรุงรักษาระบบ ตรวจสอบสถานะอุปกรณ์ อัปเดตซอฟต์แวร์ และจัดทำ Asset Inventory	บันทึกการตรวจสอบ/รายงานซ่อม/ทะเบียนครุภัณฑ์
การโจมตีทางไซเบอร์หรือข้อมูลรั่วไหล	ให้ใช้ Firewall, Antivirus, Access Control, Log Monitoring และสร้างความตระหนักด้านความปลอดภัยแก่ผู้ใช้	Log/รายงานเหตุ/บันทึกการอบรม
การสำรองข้อมูลไม่เพียงพอ	ให้กำหนดรอบ Backup/Snapshot ตรวจสอบผลสำรอง และทดสอบกู้คืนตามแผน	Backup Report/DR Test Report
บุคลากรจำกัดหรือขาดผู้ทดแทน	ให้กำหนดผู้รับผิดชอบหลักและสำรอง จัดทำคู่มือ และถ่ายทอดความรู้ภายในทีม	คู่มือ/ทะเบียนผู้รับผิดชอบ/บันทึกอบรม
กระบวนการติดตามงานล่าช้า	ให้ใช้แบบฟอร์มรับแจ้งปัญหา Dashboard หรือ Tracking Sheet เพื่อติดตามสถานะและสถิติ	ทะเบียนรับแจ้ง/รายงาน SLA/สรุปรายเดือน

14. การฟื้นฟูและการคืนสู่ภาวะปกติ

ลำดับ	การดำเนินการ	รายละเอียด
1	ยืนยันความพร้อมของระบบ	ให้ทดสอบการทำงานของระบบ บริการ เครือข่าย ฐานข้อมูล และการเข้าถึงของผู้ใช้หลัก
2	ตรวจสอบข้อมูล	ให้ตรวจสอบความครบถ้วน ถูกต้อง และช่วงเวลาข้อมูลที่กู้คืนเทียบกับ RPO
3	คืนบริการ	ให้คืนบริการตามลำดับความสำคัญ โดยเริ่มจากระบบที่กระทบภารกิจหลักก่อน
4	แจ้งผู้ใช้	ให้ประกาศสถานะคืนระบบ แนวทางการใช้งาน และข้อควรระวังหลังการฟื้นฟู
5	เฝ้าระวังหลังคืนระบบ	ให้ติดตามเสถียรภาพอย่างน้อย 24-72 ชั่วโมง หรือตามความรุนแรงของเหตุการณ์
6	สรุปบทเรียน	ให้จัดทำ Root Cause Analysis และกำหนดมาตรการป้องกันเหตุซ้ำ

15. การฝึกอบรม ทดสอบ และทบทวนแผน

กิจกรรม	ความถี่	แนวทางดำเนินการ	ผลลัพธ์ที่ต้องจัดเก็บ
ทบทวนแผน BCP-IT	อย่างน้อยปีละ 1 ครั้ง	ให้ตรวจสอบความเหมาะสมของระบบสำคัญ ผู้รับผิดชอบ ช่องทางติดต่อ และ RTO/RPO	บันทึกการทบทวน/ฉบับปรับปรุง
Tabletop Exercise	อย่างน้อยปีละ 1 ครั้ง	ให้จำลองเหตุการณ์และซักซ้อมบทบาทของผู้เกี่ยวข้อง โดยไม่กระทบระบบจริง	รายงานผลการซ้อม/ข้อเสนอปรับปรุง
ทดสอบการกู้คืนข้อมูล	อย่างน้อยปีละ 1 ครั้ง	ให้ทดสอบกู้คืนข้อมูลตัวอย่างหรือระบบที่กำหนด เพื่อยืนยันความพร้อมของ Backup/DR	DR Test Report/Backup Verification
อบรมผู้ใช้/ทีม IT	ตามความจำเป็น	ให้สื่อสารช่องทางแจ้งเหตุ แนวทางปฏิบัติด้านความปลอดภัย และบทบาทเมื่อเกิดเหตุ	ทะเบียนอบรม/สื่อประกอบ
ทบทวนหลังเหตุการณ์จริง	ทุกครั้งที่เกิดเหตุสำคัญ	ให้วิเคราะห์สาเหตุ ผลกระทบ ความสำเร็จ ข้อบกพร่อง และมาตรการป้องกันซ้ำ	รายงาน Post-Incident Review

16. ตัวชี้วัดการดำเนินงาน

ตัวชี้วัด	เป้าหมายเบื้องต้น	วิธีติดตาม
Uptime ของระบบสำคัญ	ไม่น้อยกว่า 99.5% ต่อไตรมาส หรือตามความพร้อมของระบบ	Monitoring Report/Dashboard
MTTD (Mean Time to Detect)	เหตุวิกฤติไม่เกิน 15 นาที เมื่อมีระบบ Monitoring รองรับ	บันทึกเวลาแจ้งเตือน/รับแจ้งเหตุ
MTTR (Mean Time to Restore)	เหตุวิกฤติให้กู้คืนบริการหลักไม่เกิน 2-4 ชั่วโมงตามประเภทระบบ	Incident Report
การทดสอบกู้คืนข้อมูล	อย่างน้อยปีละ 1 ครั้ง	รายงาน DR Test/Backup Test
เหตุซ้ำจากสาเหตุเดิม	ลดลงเมื่อเทียบกับรอบประเมินก่อนหน้า	รายงาน Root Cause/สถิติรายเดือน

17. การรายงานและการจัดเก็บหลักฐาน

เมื่อเกิดเหตุขัดข้อง ให้บันทึกข้อมูลและจัดเก็บหลักฐานอย่างน้อยตามรายการต่อไปนี้ เพื่อใช้ประกอบการรายงาน การทบทวน และการปรับปรุงแผน

รายการหลักฐาน	รายละเอียดที่ต้องมี
แบบบันทึกเหตุการณ์	วันเวลา ผู้แจ้ง ระบบที่กระทบ อาการ ระดับความรุนแรง ผู้รับผิดชอบ และสถานะงาน
Log และหลักฐานเทคนิค	System Log, Network Log, Security Log, ภาพหน้าจอ หรือข้อมูลประกอบอื่นที่เกี่ยวข้อง
รายงานการแก้ไข	สาเหตุ วิธีแก้ไข ระยะเวลา ผลการทดสอบ และผู้อนุมัติคืนระบบ
รายงานหลังเหตุการณ์	ผลกระทบ บทเรียน ข้อเสนอปรับปรุง และมาตรการป้องกันเหตุซ้ำ
หลักฐานการสื่อสาร	ข้อความแจ้งผู้ใช้ รายงานผู้บริหาร หรือประกาศสถานะระบบ

18. ภาคผนวก ก : แบบบันทึกเหตุการณ์ขัดข้องด้าน IT

หัวข้อ	รายละเอียด
วันที่/เวลาเริ่มเหตุ	.....
ช่องทางรับแจ้ง	☐ QR Code ☐ Line ☐ Email ☐ โทรศัพท์ ☐ แจ้งโดยตรง
ชื่อผู้แจ้ง/หน่วยงาน	.....
ระบบหรืออุปกรณ์ที่ได้รับผลกระทบ	.....
อาการ/ผลกระทบ	.....
ระดับเหตุการณ์	☐ Critical ☐ High ☐ Medium ☐ Low
ผู้รับผิดชอบดำเนินการ	.....
แนวทางแก้ไขเบื้องต้น	.....
วันที่/เวลาคืนระบบ	.....
ผลการทดสอบหลังแก้ไข	.....

19. ภาคผนวก ข : Checklist การตอบสนองเหตุขัดข้อง

ลำดับ	รายการตรวจสอบ	สถานะ
1	รับแจ้งเหตุและบันทึกรายละเอียดครบถ้วน	☐ ดำเนินการแล้ว ☐ ยังไม่ดำเนินการ
2	ประเมินระดับความรุนแรงและผลกระทบ	☐ ดำเนินการแล้ว ☐ ยังไม่ดำเนินการ
3	แจ้งหัวหน้างาน/ผู้บริหารตามระดับเหตุการณ์	☐ ดำเนินการแล้ว ☐ ยังไม่ดำเนินการ
4	จำกัดขอบเขตของปัญหาและป้องกันผลกระทบต่อระบบอื่น	☐ ดำเนินการแล้ว ☐ ยังไม่ดำเนินการ
5	ตรวจสอบ Log ระบบ เครือข่าย Server Storage และอุปกรณ์ที่เกี่ยวข้อง	☐ ดำเนินการแล้ว ☐ ยังไม่ดำเนินการ
6	ดำเนินการแก้ไขหรือเปิดใช้ระบบ/ช่องทางสำรอง	☐ ดำเนินการแล้ว ☐ ยังไม่ดำเนินการ
7	ทดสอบระบบก่อนคืนบริการ	☐ ดำเนินการแล้ว ☐ ยังไม่ดำเนินการ
8	แจ้งผู้ใช้และผู้บริหารเมื่อคืนระบบแล้ว	☐ ดำเนินการแล้ว ☐ ยังไม่ดำเนินการ

ลำดับ	รายการตรวจสอบ	สถานะ
9	จัดทำรายงานหลังเหตุการณ์และข้อเสนอป้องกันเหตุซ้ำ	☐ ดำเนินการแล้ว ☐ ยังไม่ดำเนินการ