(ร่าง) แผนความเสี่ยงและความต่อเนื่องทางธุรกิจ
ด้านเทคโนโลยีสารสนเทศ
(Business Continuity Plan: BCP)

บทนำ

ในยุคที่เทคโนโลยีสารสนเทศมีบทบาทสำคัญต่อการดำเนินงานขององค์กร การพึ่งพาระบบสารสนเทศในการจัดเก็บข้อมูล การสื่อสาร และการให้บริการต่าง ๆ ได้เพิ่มขึ้นอย่างต่อเนื่อง อย่างไรก็ตาม ความเสี่ยงจากภัยคุกคามทั้งจากภายในและภายนอก เช่น ความผิดพลาดของระบบ การโจมตีทางไซเบอร์ หรือภัยธรรมชาติ อาจส่งผลให้ระบบสารสนเทศไม่สามารถใช้งานได้ตามปกติ ซึ่งอาจกระทบต่อความต่อเนื่องในการดำเนินงานขององค์กรอย่างรุนแรง เพื่อเตรียมความพร้อมรับมือกับเหตุการณ์ไม่คาดคิด และลดผลกระทบที่อาจเกิดขึ้น องค์กรจึงจำเป็นต้องจัดทำ แผนความเสี่ยงและความต่อเนื่องทางธุรกิจด้านเทคโนโลยีสารสนเทศ (Business Continuity Plan : BCP) ขึ้น โดยมีวัตถุประสงค์เพื่อกำหนดแนวทาง ขั้นตอน และมาตรการในการฟื้นฟูระบบสารสนเทศให้กลับมาใช้งานได้อย่างรวดเร็วและปลอดภัย รวมถึงการรักษาความมั่นคงของข้อมูลและความเชื่อมั่นของผู้ใช้บริการ แผนนี้จะครอบคลุมการประเมินความเสี่ยง การจัดลำดับความสำคัญของระบบ การกำหนดระยะเวลาในการกู้คืน การจัดเตรียมทรัพยากรสำรอง และการฝึกอบรมบุคลากร เพื่อให้มั่นใจว่าองค์กรสามารถตอบสนองต่อเหตุการณ์ฉุกเฉินได้อย่างมีประสิทธิภาพ และสามารถดำเนินงานได้อย่างต่อเนื่อง

สารบัญ

เรื่อง

วัตถุประสงค์ของการจัดทำแผนความเสี่ยงและความต่อเนื่องทางธุรกิจด้านเทคโนโลยีสารสนเทศ (BCP) 1

คำนิยามในแผนความเสี่ยงและความต่อเนื่องทางธุรกิจด้านเทคโนโลยีสารสนเทศ (Business Continuity Plan: BCP) 1

ขั้นตอนและแผนความเสี่ยงและความต่อเนื่องทางธุรกิจด้านเทคโนโลยีสารสนเทศ (BCP) 2

การประเมินความเสี่ยงและผลกระทบ (Risk & Impact Assessment) 2

การจัดลำดับความสำคัญของระบบสารสนเทศ (System Prioritization) 4

กำหนด Recovery Time Objective (RTO) และ Recovery Point Objective (RPO) 4

การจัดเตรียมทรัพยากรสำรอง(Backup & Redundancy) 5

การจัดทำแผนปฏิบัติการ (Recovery Procedures) 6

การทดสอบแผน (Testing & Simulation) 11

การเฝ้าระวัง ติดตามการดำเนินงาน และการรายงานผล 12

ฝึกอบรมบุคลากร (Training) 13

วัตถุประสงค์ของการจัดทำแผนความเสี่ยงและความต่อเนื่องทางธุรกิจด้านเทคโนโลยีสารสนเทศ (BCP)

1. เพื่อเตรียมความพร้อมในการรับมือกับเหตุการณ์ไม่คาดคิด จากการโจมตีทางไซเบอร์, ความผิดพลาดของระบบ หรือความผิดพลาดจากมนุษย์
2. เพื่อกำหนดแนวทางและขั้นตอนในการฟื้นฟูระบบสารสนเทศ ให้สามารถกลับมาใช้งานได้อย่างรวดเร็ว ปลอดภัย และมีประสิทธิภาพ
3. เพื่อรักษาความต่อเนื่องในการดำเนินงานขององค์กร ลดผลกระทบที่อาจเกิดขึ้นต่อการให้บริการและการบริหารจัดการภายในองค์กร
4. เพื่อปกป้องข้อมูลสำคัญและลดความเสี่ยงจากการสูญหายของข้อมูล โดยการจัดทำระบบสำรองข้อมูลและมาตรการรักษาความมั่นคงปลอดภัยของข้อมูล
5. เพื่อกำหนดบทบาทและความรับผิดชอบของบุคลากรในภาวะวิกฤต ให้สามารถดำเนินการตามแผนได้อย่างเป็นระบบและมีประสิทธิภาพ

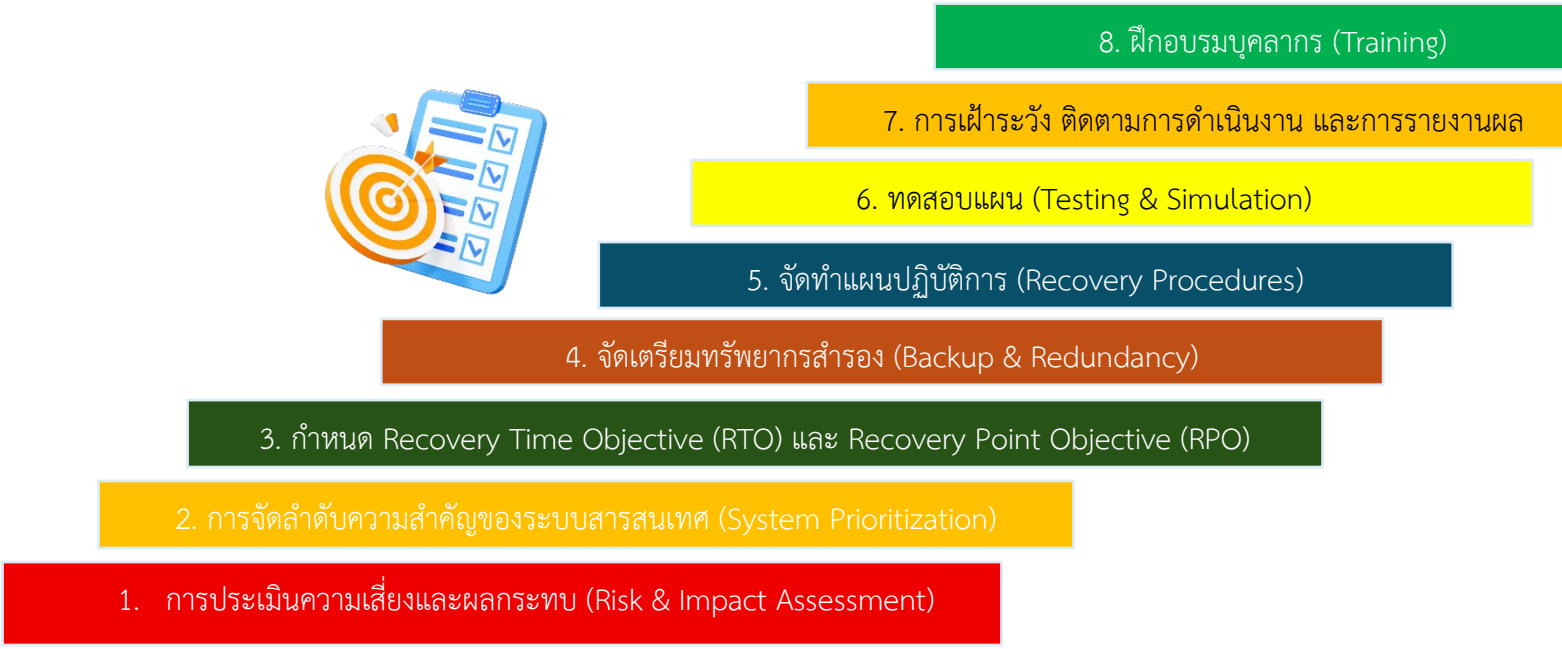
โดยมีเป้าหมายกู้คืนระบบสารสนเทศต้องดำเนินการกู้คืนบริการให้เสร็จภายในระยะเวลาตามที่กำหนดไว้ในตารางที่ 1-1 ....

คำนิยามในแผนความเสี่ยงและความต่อเนื่องทางธุรกิจด้านเทคโนโลยีสารสนเทศ (Business Continuity Plan : BCP)

1. **ผู้บัญชาการสูงสุด** – ผู้บริหารเทคโนโลยีสารสนเทศระดับสูง ประจำสถาบันพระบรมราชชนก (DCIO)
2. **แผน BCP** – แผนความเสี่ยงและความต่อเนื่องทางธุรกิจด้านเทคโนโลยีสารสนเทศ (Business Continuity Plan: BCP)
3. **Recovery Time Objective (RTO)** - ระยะเวลาหลังเกิดเหตุการณ์ที่ธุรกิจต้องกลับมาดำเนินงานได้ หรือ ระยะเวลาฟื้นฟูธุรกิจ
4. **Minimum Business Continuity Objective (MBCO)** - ระดับบริการหรือการผลิตขั้นต่ำที่องค์กรต้องการบรรลุเพื่อให้สามารถดำเนินงานและให้บริการลูกค้าได้ในระดับที่ยอมรับได้ในช่วงเวลาที่เกิดเหตุการณ์หยุดชะงักหรือภัยพิบัติ
5. **Recovery Point Objective (RPO)** - เวลาที่ย้อนกลับไป โดยหากเกิดเหตุการณ์ไม่คาดฝัน
6. ศูนย์คอมพิวเตอร์สำรอง **PBRI_DR -** ศูนย์คอมพิวเตอร์สำรอง ณ สถาบันพระบรมราชชนก อาคาร 6 ชั้น 9
7. ศูนย์คอมพิวเตอร์สำรอง **GDCC_DR -** ศูนย์คอมพิวเตอร์สำรอง ณ ระบบคลาวด์กลางภาครัฐ กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม

8. ทีมกู้คืนบริการ – บคลากรที่ได้รับมอบหมายให้รับผิดชอบในการกู้คืนระบบสารสนเทศ ทั้งที่เป็นบุคลากรในสังกัด หรือ หน่วยงานภายนอก
9. เจ้าหน้าที่รับแจ้งเหตุการณ์ความมั่นคงปลอดภัย - ทำหน้าที่รับแจ้งและบันทึกเหตุการณ์ความมั่นคงปลอดภัย (ทั้งเหตุการณ์ภัยพิบัติและเหตุหยุดชะงัก), วิเคราะห์และประเมินเหตุการณ์ที่ได้รับ แจ้งว่ามีความรุนแรงในระดับใด, และประสานงานแจ้งเหตุการณ์ที่ได้รับแจ้งให้ หัวหน้าทีมกู้คืนระบบ เลขาทีมกู้คืนระบบ และทีมกู้คืนระบบ ผู้บัญชาการสูงสุด ได้รับทราบ

ขั้นตอนและแผนความเสี่ยงและความต่อเนื่องทางธุรกิจด้านเทคโนโลยีสารสนเทศ (Business Continuity Plan : BCP)



การประเมินความเสี่ยงและผลกระทบ (Risk & Impact Assessment)

สามารถ ประเมินความเสี่ยงและแบ่งระดับความสำคัญตามความรุนแรง และผลกระทบของเหตุการณ์แบ่งได้เป็น 3 ระดับดังนี้

<u>ระดับที่ 1 : เหตุการณ์ทั่วไป (Minor)</u>

เป็นเหตุการณ์ทั่วไปซึ่งเกิดขึ้น และมีผลกระทบเล็กน้อยต่อ สถาบันพระบรมราชชนก สามารถแก้ไขได้โดยใช้วิธีการ และทรัพยากรของสถาบันพระบรมราชชนกที่มีอยู่ ไม่ต้องการความช่วยเหลือจากภายนอก มีผลกระทบเล็กน้อยต่อ กระบวนการสำคัญของสถาบันพระบรม

ราชชนก ไม่มีการเรียกใช้แผนการบริหารจัดการ เหตุการณ์ความมั่นคงปลอดภัย กรณีระบบงานของสถาบันพระบรมราชชนกเกิดการหยุดชะงัก ซึ่งเป็นปัญหาประจำวันที่เกิดขึ้น อยู่เป็นครั้งคราว และใช้ระยะเวลาไม่นานในการแก้ไข ระบบก็จะกลับคืนมาให้บริการถือเป็นเหตุการณทั่วไป ตัวอย่างเหตุการณ์ ได้แก่ กระบวนการสำคัญหยุดชะงักในเวลาสั้นๆ ไฟฟ้าดับในอาคารชั่วคราว ท่อประปาในอาคารแตก การบาดเจ็บจากการถูกของมีคมบาด ระบบงานหยุดชะงักในระยะเวลาสั้น ๆ เป็นต้น

<u>ระดับที่ 2 : เหตุการณ์รุนแรง (Major)</u>

เป็นเหตุการณ์รุนแรงซึ่งเกิดขึ้น และมีผลกระทบในวงกว้าง ต่อสถาบันพระบรมราชชนก ซึ่งสามารถแก้ไขได้ โดยใช้วิธีการ และทรัพยากรของสถาบันพระบรมราชชนกมีอยู่ แต่อาจจำเป็นต้องได้รับความช่วยเหลือจากหน่วยงานภายนอก (เช่น การไฟฟ้า การประปา หน่วยดับเพลิง หน่วยกู้ภัย) เหตุการณ์อาจมีการขยายตัว ยืดเยื้อ ลุกลาม หรือ ขยายขอบเขตออกไปได้ และส่งผลกระทบอย่างมากต่อกระบวนการสำคัญ (ซึ่งรวมถึงการหยุดชะงักของกระบวนการด้วย) และ/หรือ ชีวิตและความปลอดภัยของผู้ที่เกี่ยวข้องในสถาบันพระบรมราชชนกเหตุการณ์ประเภทนี้จะมีการเรียกใช้แผนการบริหารจัดการนี้ กรณีระบบงานสำคัญเกิดการหยุดชะงักและจำเป็นต้องใช้ระยะเวลานานในการแก้ไข ซึ่งอาจจำเป็น ต้องเปลี่ยนมาไปใช้ระบบสำรองแทน ที่อาจติดตั้งเอาไว้แล้วหรือต้องจัดหาหรือสรรหาเพิ่มเติม มาใช้งานก็ตาม กรณีนี้ก็ถือเป็นเหตุการณ์รุนแรง ตัวอย่างเหตุการณ์ ได้แก่ กระบวนการสำคัญหยุดชะงักในระยะเวลายาวนาน ไฟฟ้าดับทั้งหมด เป็นระยะเวลานาน หม้อแปลงไฟฟ้าแรงสูงที่จ่ายไฟเข้าสถาบันพระบรมราชชนก ระเบิดไฟไหม้และลุกลามไปยังหลายหน่วยงานภายในสำนักงาน ระบบสาธารณูปโภคใช้งานไม่ได้เป็นระยะเวลานาน การปิดล้อมโดยฝูงชนที่มีการยืดเยื้อ น้ำท่วมขังรอบสถาบันพระบรมราชชนกในระยะเวลาไม่นานนัก ระบบงานสำคัญหยุดชะงักเป็นระยะเวลานาน

<u>ระดับที่ 3 : เหตุการณ์หายนะ (Crisis)</u>

เป็นเหตุการณ์หายนะซึ่งเกิดขึ้น และมีผลกระทบทั่วทั้ง สถาบันพระบรมราชชนกและสังคมแวดล้อม เหตุการณ์ประเภทนี้จำเป็นอย่างยิ่งที่ต้องได้รับความช่วยเหลือ และประสานงานกับหน่วยงานภายนอก เหตุการณ์มีผลกระทบอย่างสูงต่อกระบวนการสำคัญ หลายกระบวนการหรือทั้งหมด และ/หรือ ชีวิตและความปลอดภัยของผู้ที่เกี่ยวข้องและสังคมแวดล้อม ของสถาบันพระบรมราชชนก กรณีระบบงานสำคัญหลายระบบหรือทั้งหมดเกิดการหยุดชะงัก และจำเป็นต้องใช้ระยะเวลานานในการแก้ไข ซึ่งอาจจะเป็นต้องเปลี่ยนไปใช้ระบบสำรองแทน ที่อาจติดตั้งเอาไว้แล้ว หรือต้อง จัดหาหรือสรรหาเพิ่มเติมมาใช้งานก็ตาม กรณีนี้ก็ถือเป็นเหตุการณ์หายนะ ตัวอย่างเหตุการณ์ ได้แก่ กระบวนการสำคัญหลายกระบวนการหรือทั้งหมดหยุดชะงัก ไฟไหม้กับพื้นที่ส่วนใหญ่ของสถาบันพระบรมราชชนก แผ่นดินไหว น้ำท่วมขังเป็น ระยะเวลาต่อเนื่องและยาวนานหลายสัปดาห์ สงคราม ระบบงานสำคัญหลายระบบหรือทั้งหมดหยุดชะงักเป็น ระยะเวลานาน เกิดการแพร่ระบาดของโรคติดเชื้ออุบัติใหม่

การจัดลำดับความสำคัญของระบบสารสนเทศ (System Prioritization)

สถาบันพระบรมราชชนก วิเคราะห์และจัดลำดับความสำคัญของระบบสารสนเทศ และ ระบบบริการต่างๆ โดยใช้ข้อมูลผลกระทบและเป้าหมายการกู้คืนเป็นตัวกำหนด ตามรางที่ 1-2 การจัดลำดับความสำคัญของระบบสารสนเทศ และ กำหนด Recovery Time Objective (RTO) และ Recovery Point Objective (RPO)

กำหนด Recovery Time Objective (RTO) และ Recovery Point Objective (RPO)

เวลาที่ระบบต้องกลับมาใช้งานได้ Recovery Time Objective (RTO) และข้อมูลล่าสุดที่สามารถยอมรับได้ในการกู้คืน Recovery Point Objective (RPO) ตามรางที่ 1-2 การจัดลำดับความสำคัญของระบบสารสนเทศ และ กำหนด Recovery Time Objective (RTO) และ Recovery Point Objective (RPO)

ID	ระบบสารสนเทศ/Service	Recovery Time Objective (RTO)	Minimum Business Continuity Objective (MBCO)	Recovery Point Objective (RPO)
1	ระบบสารบรรณอิเล็กทรอนิกส์ (E-Saraban) ไว้บน GDCC	4 ชม.	ระบบงานมีขีดความสามารถที่ร้อยละ 70 เมื่อเทียบกับระบบหลัก	1 วัน
2	ระบบบริหารทรัพยากรบุคคล (Human Resource Information System: HRIS)	4 ชม.	ระบบงานมีขีดความสามารถที่ร้อยละ 70 เมื่อเทียบกับระบบหลัก	1 วัน
3	ระบบชำระเงินออนไลน์ (E-Billing) ไว้ที่ server สบช.ก่อน	4 ชม.	ระบบงานมีขีดความสามารถที่ร้อยละ 70 เมื่อเทียบกับระบบหลัก	1 วัน
4	ระบบลงทะเบียนอบรม บริการวิชาการ ไว้ที่ server สบช.ก่อน	4 ชม.	ระบบงานมีขีดความสามารถที่ร้อยละ 70 เมื่อเทียบกับระบบหลัก	1 วัน
5	ระบบรับสมัครและคัดเลือกนักศึกษาใหม่ สถาบันพระบรมราชชนก	4 ชม.	ระบบงานมีขีดความสามารถที่ร้อยละ 70 เมื่อเทียบกับระบบหลัก	1 วัน
6	ระบบคลังข้อสอบและการสอบออนไลน์ ไว้ที่ server สบช.ก่อน	4 ชม.	ระบบงานมีขีดความสามารถที่ร้อยละ 70 เมื่อเทียบกับระบบหลัก	4 ชม.
7	ระบบจองประชุม ไว้บน GDCC	1 ชม.	ระบบงานมีขีดความสามารถที่ร้อยละ 70 เมื่อเทียบกับระบบหลัก	1 วัน
8	ระบบจองรถ ไว้บน GDCC	1 ชม.	ระบบงานมีขีดความสามารถที่ร้อยละ 70 เมื่อเทียบกับระบบหลัก	1 วัน

ID	ระบบสารสนเทศ/Service	Recovery Time Objective (RTO)	Minimum Business Continuity Objective (MBCO)	Recovery Point Objective (RPO)
9	เว็บไซต์ สถาบันพระบรมราชชนก ไว้บน GDCC	4 ชม.	ระบบงานมีขีดความสามารถที่ ร้อยละ 90 เมื่อเทียบกับระบบหลัก	4 ชม.
10	ระบบการเรียนการสอนออนไลน์ (SPOC) ไว้ที่ server สบช.ก่อน	4 ชม.	ระบบงานมีขีดความสามารถที่ ร้อยละ 70 เมื่อเทียบกับระบบหลัก	1 วัน

ตารางที่ 1-2 การจัดลำดับความสำคัญของระบบสารสนเทศ และ กำหนด Recovery Time Objective (RTO) และ Recovery Point Objective (RPO)

การจัดเตรียมทรัพยากรสำรอง(Backup & Redundancy)

ในการกู้คืนระบบสารสนเทศจะต้องอาศัยการทำงานของอุปกรณ์ต่าง ๆ ในศูนย์คอมพิวเตอร์ เช่น เครื่องปรับอากาศ เครื่องสำรองไฟ ฯลฯ กรณีที่อุปกรณ์เหล่านี้เกิดความเสียหายทางกายภาพ ทีมกู้คืนจำเป็นต้องอาศัยผู้ให้บริการภายนอกตามที่ปรากฏในตารางด้านล่างนำอุปกรณ์มาเปลี่ยนทดแทนอุปกรณ์ที่เกิดความเสียหายนั้น ตามตาราง ที่ 1-3 ทรัพยากรสำรองจากหน่วยงานภายนอก

หน่วยงานภายนอก	Dependency	หมายเหตุ
ผู้ให้บริการ MA Network	MA, PM, ห้อง DATA CENTER SLA ตามสัญญา	- DATA CENTER ตามสัญญา - แก้ไขปัญหาอุปกรณ์เครื่องแม่ข่ายและเครือข่ายตามสัญญา
ผู้ให้บริการ Cloud DR	เตรียมอุปกรณ์ HW, SW, Link สัญญาณ ดังตารางที่ 3	Contract in place
บริษัท โทรคมนาคมแห่งชาติ จำกัด (มหาชน)	บริการ Internet เมื่อเกิดเหตุมี Link สำรองให้	SLA ตามสัญญา
บริษัท แอดวานซ์ อินโฟร์ เซอร์วิส จำกัด (มหาชน)	บริการ Internet เมื่อเกิดเหตุมี Link สำรองให้	SLA ตามสัญญา
การไฟฟ้าส่วนภูมิภาค	จ่ายกระแสไฟฟ้ามีระบบไฟฟ้าสำรอง	ตามสัญญา

ตามรางที่ 1-3 ทรัพยากรสำรองจากหน่วยงานภายนอก

การจัดทำแผนปฏิบัติการ (Recovery Procedures)

1. เพื่อให้เจ้าหน้าที่สามารถดำเนินการได้อย่างเป็นระบบ ลดความสับสนและความผิดพลาดในภาวะวิกฤต กำหนดบทบาทและความรับผิดชอบของแต่ละฝ่าย เพื่อให้การกู้คืนเป็นไปตามลำดับความสำคัญของระบบ สถาบันพระบรมราชชนก กำหนดแผน และ ผู้รับผิดชอบดังนี้ ตารางที่ 1-4 การดำเนินการตามลำดับขั้นตอนแผนความเสี่ยงและความต่อเนื่องทางธุรกิจด้านเทคโนโลยีสารสนเทศ และตารางที่ 1-5 ทีมกู้คืน บทบาท และหน้าที่ความรับผิดชอบ

ขั้นตอน	คำอธิบาย	การสั่งการของผู้มีอำนาจ
1.การประเมินสถานการณ์	ตรวจสอบเหตุการณ์ที่เกิดขึ้น เช่น ระบบล่ม, ข้อมูลสูญหาย, หรือภัยธรรมชาติ เพื่อประเมินความรุนแรงและขอบเขตของผลกระทบ	ผู้บริหารหรือหัวหน้าหน่วยงานเป็นผู้ตัดสินใจว่าเหตุการณ์นั้นเข้าข่ายภาวะวิกฤต และอนุมัติให้เริ่มใช้แผน BCP
2.การแจ้งเตือนและสื่อสารภายใน	แจ้งเหตุการณ์ไปยังผู้เกี่ยวข้อง เช่น ทีม IT,ผู้บริหารระดับสูง,และหน่วยงานที่ได้รับผลกระทบ เพื่อเตรียมความพร้อม	ผู้มีอำนาจกำหนดช่องทางการสื่อสาร เช่น อีเมล, โทรศัพท์, หรือระบบแจ้งเตือน และแต่งตั้งผู้ประสานงานกลาง
3.การวิเคราะห์ผลกระทบและลำดับความสำคัญ	ประเมินระบบที่ได้รับผลกระทบ และจัดลำดับความสำคัญของระบบที่ต้องกู้คืนก่อน เช่น ระบบฐานข้อมูล, ระบบบริการผู้ใช้	ผู้บริหารร่วมกับทีมเทคนิคตัดสินใจลำดับการกู้คืน โดยพิจารณาจากผลกระทบต่อภารกิจหลักขององค์กร
4.การดำเนินการกู้คืนระบบ	เริ่มกระบวนการกู้คืน เช่น ใช้ข้อมูลสำรอง,เปลี่ยนไปใช้ระบบสำรอง,หรือย้ายการทำงานไปยังศูนย์สำรอง	ผู้มีอำนาจอนุมัติการใช้ทรัพยากรสำรอง เช่น งบประมาณ, บุคลากร, หรืออุปกรณ์สำรอง และติดตามความคืบหน้า
5.การตรวจสอบและทดสอบระบบหลังการกู้คืน	ตรวจสอบความถูกต้องของระบบและข้อมูลหลังการกู้คืนเพื่อให้มั่นใจว่าระบบสามารถกลับมาใช้งานได้ตามปกติ	ผู้บริหารรับรองผลการกู้คืน และอนุมัติให้เปิดระบบกลับมาให้บริการตามปกติ
6.การรายงานและปรับปรุงแผน	สรุปเหตุการณ์และผลการดำเนินงานพร้อมปรับปรุงแผน BCP ให้มีประสิทธิภาพมากขึ้นในอนาคต	ผู้บริหารสั่งการให้จัดทำรายงานสรุปและกำกับให้มี การปรับปรุงแผนตามบทเรียนที่ได้รับ

ตารางที่ 1-4 การดำเนินการตามลำดับขั้นตอนแผน BCP

ลำดับ	ชื่อ	บทบาทและหน้าที่ความรับผิดชอบ
1	หัวหน้าทีมกู้คืนระบบ	
	ผู้อำนวยการ กองเทคโนโลยีดิจิทัล (นายดุลยวัฒน์ มาป้อง)	1. ประเมินสถานการณ์ที่เกิดขึ้นว่ามีผลกระทบ และความ รุนแรงในระดับใด 2. ระดมลูกทีมทั้งหมดเพื่อลงพื้นที่ปฏิบัติการ ประสานงาน และสั่งการให้ลูกทีมร่วมกันดำเนินการแก้ไขปัญหาที่พบ 3. รายงานสถานการณ์การกู้คืนระบบให้หน่วยติดตาม สถานการณ์ ให้ผู้บัญชาการสูงสุด ได้รับทราบอย่างเป็นระยะ ๆ 4. ประสานงานกับฝ่ายอาคารสถานที่ เพื่อ ขอให้ช่วยดำเนินการในเรื่องต่าง ๆ อาทิ ตรวจสอบ ระบบไฟฟ้า ระบบโทรศัพท์ ระบบปรับอากาศ การรักษาความปลอดภัย หรืออื่น ๆ ที่เกี่ยวข้อง 5. สั่งการให้ลูกทีมตรวจสอบและเตรียมความพร้อมของ ระบบเทคโนโลยีสารสนเทศต่างๆ ในศูนย์คอมพิวเตอร์สำรอง PBRI_DR และ GDCC_DR 6. จัดทำรายงาน After Action Report ภายหลัง สถานการณ์สิ้นสุดลง
2	ทีมติดตั้งเซิร์ฟเวอร์และเครือข่าย	
	1. ว่าที่เรือตรียุทธชัย สุนทรวิภาต 2. นายธชา ศรีนวลขาว 3. นายพีรวัส สุทัตโต 4. นายนัฐกานต์ เคหาวิตร	1. สำรวจและประเมินความเสียหายของฮาร์ดแวร์ อุปกรณ์ ข้อมูล และ/หรือซอฟต์แวร์ต่าง ๆ ของระบบที่เกิดความ เสียหาย และจำเป็นต้องแก้ไขหรือติดตั้งกลับคืน 2. กำหนดรายการของฮาร์ดแวร์ อุปกรณ์ ข้อมูล และ/หรือ ซอฟต์แวร์ต่าง ๆ ที่จำเป็นต้องใช้ในการกู้คืน 3. แจ้งรายการฮาร์ดแวร์หรืออุปกรณ์ที่ต้องการ พร้อมทั้ง คุณลักษณะให้ทีมการจัดการทั่วไป ช่วยดำเนินการ จัดหาให้ 4. ติดตั้งฮาร์ดแวร์ อุปกรณ์ และ/หรือซอฟต์แวร์ที่เกี่ยวข้อง กับระบบโดยติดตั้งให้เหมือนเดิม หรือใกล้เคียงกับ ระบบเดิมให้มากที่สุด 5. นำข้อมูลล่าสุดที่สำรองเก็บไว้มาทำการติดตั้งกลับคืน ตามความจำเป็น
3	ทีมติดตั้งแอปพลิเคชันและฐานข้อมูล	
	1. นางสาวน้ำฝน เอี่ยมวิริยาวัฒน์ 2. นายธชา ศรีนวลขาว 3. นายเจตรินทร์ ทัดปากน้ำ 4. นางสาวพิชญาดา กฤตเวทิน	1. ติดตั้งและปรับแต่ง Application ให้เหมือนระบบเดิม มากที่สุด 2. ทดสอบฟังก์ชั่นการทำงานต่าง ๆ ของระบบ เพื่อดูว่า สามารถใช้งานได้ครบถ้วนหรือไม่ 3. นำข้อมูลล่าสุด (ของฐานข้อมูล) ที่สำรองเก็บไว้มาทำ การติดตั้งกลับคืนตามความจำเป็น 4. พยายามกู้คืนข้อมูลของระบบ ให้กลับไปสู่จุดเวลาที่เกิด เหตุหยุดชะงักขึ้น 5. ตรวจสอบดูความถูกต้องของข้อมูลที่ทำการติดตั้ง กลับคืนนั้น เท่าที่ทำได้ 6. ทดสอบระบบร่วมกับผู้ใช้งาน
4	ทีมประชาสัมพันธ์	

ลำดับ	ชื่อ	บทบาทและหน้าที่ความรับผิดชอบ
	1. นางสาวอุบลรัตน์ เทศนาบูรณ์ 2. นายกษิเดช เศรษฐวนิช	1 รับแจ้งเหตุสอบถาม เพื่อรวบรวมข้อมูลอย่างน้อยดังนี้ • เหตุการณ์ที่เกิด • ชื่อผู้แจ้งเหตุ • หน่วยงานของผู้แจ้งเหตุ • เบอร์โทรศัพท์ติดต่อกลับ • วัน/เวลาที่พบ • สถานที่ที่พบเหตุ • รายละเอียดของเหตุการณ์ เช่น ความเสียหายที่เกิดขึ้น 2. สื่อสารภายในองค์กร 3. สื่อสารภายนอกองค์กร

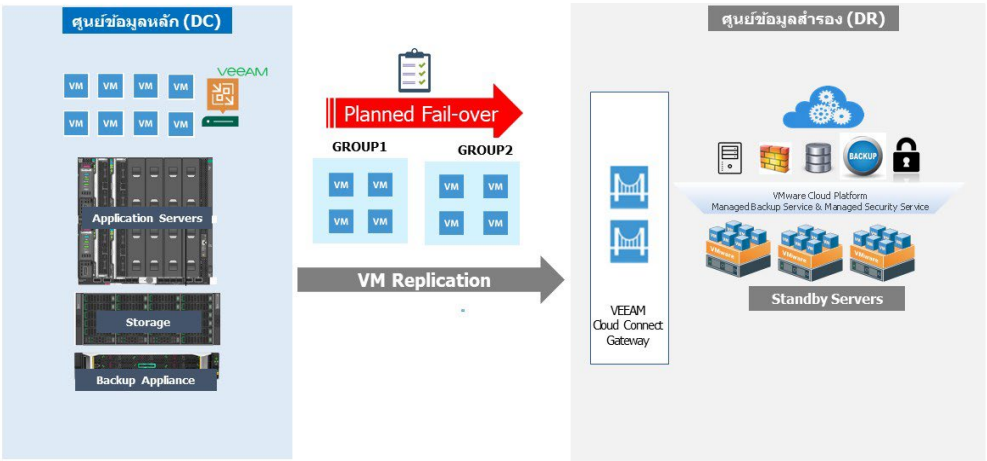
ตารางที่ 1-5 ทีมกู้คืนบริการ บทบาท และหน้าที่ความรับผิดชอบ

ขั้นตอนการกู้คืนบริการระบบสารสนเทศ

ขั้นตอนนี้เป็นการกู้คืนบริการระบบสารสนเทศ ณ ที่ไซต์สำรองตามที่กำหนดไว้ เพื่อให้สามารถกลับคืนมาให้บริการได้ตามระยะเวลาเป้าหมายของการกู้คืนที่กำหนดไว้

ในรูปฝั่งขวามือคือศูนย์คอมพิวเตอร์สำรอง PBRI_DR และ GDCC_DR ของบริการระบบสารสนเทศ ซึ่งได้มีการเตรียมการ เซิร์ฟเวอร์ และอุปกรณ์ต่าง ๆ ตาม ที่ปรากฏในรูป เพื่อให้สามารถกู้คืนบริการให้กลับคืนมาให้บริการได้ ตามปกติ

แผนภาพแสดงการทำแผนรองรับภัยพิบัติและสถานการณ์ฉุกเฉิน (Business Continuity Plan)



ความต้องการด้านทรัพยากรในการกู้คืนบริการระบบสารสนเทศ

ทรัพยากรที่จำเป็นต้องใช้สำหรับการกู้คืนบริการระบบสารสนเทศ ตาม ตารางที่ 1-6 ความต้องการด้านทรัพยากรของแผนความเสี่ยงและความต่อเนื่องทางธุรกิจด้านเทคโนโลยีสารสนเทศ

ทรัพยากรที่ต้องใช้	จำนวน	แหล่งในการจัดหา	หมายเหตุ
อุปกรณ์ป้องกันเครือข่าย (Fortinet FortiGate)	1	ของสถาบันฯ	
อุปกรณ์กระจายสัญญาณ (L3 Switch 10 Gigabit Ethernet)	2	ของสถาบันฯ	
อุปกรณ์กระจายสัญญาณไร้สาย (Wireless Access Point)	5	ของสถาบันฯ	
เครื่องคอมพิวเตอร์แม่ข่าย (CPU 22 Core, Memory 256 GB, SSD 7.68 TB)	4	ของสถาบันฯ	
ชุดโปรแกรม Hypervisor Software	1	ของสถาบันฯ	
อุปกรณ Veritas Backup	1	ของสถาบันฯ	
สัญญาญ Link Internet 2 Gbps	1	ของสถาบันฯ	
VPN	100	ของสถาบันฯ	

ตารางที่ 1-6 ความต้องการด้านทรัพยากรของแผน BCP

Checklist ของการกู้คืนบริการระบบสารสนเทศ ดังปรากฏใน ตาราง 1-7 Checklist ของการกู้คืนบริการระบบสารสนเทศ ด้านล่าง

	งานที่ต้องทำ	อ้างอิงขั้นตอนปฏิบัติ	ระยะเวลาที่ใช้ในการดำเนินการ	ระยะเวลาที่ทำได้จริง	ลายมือชื่อของผู้ดำเนินการ
การเตรียมความพร้อมของระบบสำรอง					
1.	ทีมกู้คืนบริการ ตรวจสอบความพร้อมใช้ของระบบเครือข่ายที่ศูนย์คอมพิวเตอร์สำรอง และดำเนินการตามที่เห็นสมควร เพื่อให้ระบบเครือข่ายพร้อม ที่จะใช้งานได้				

งานที่ต้องทำ		อ้างอิงขั้นตอนปฏิบัติ	ระยะเวลาที่ใช้ในการดำเนินการ	ระยะเวลาที่ทำได้จริง	ลายมือชื่อของผู้ดำเนินการ
2.	ทีมกู้คืนบริการ และ/หรือ ผู้ให้บริการภายนอก ร่วมกันจัดเตรียมระบบสำรองให้พร้อมใช้งาน โดยดำเนินการดังนี้ ● ดำเนินการ Restore ข้อมูลที่ได้ทำการ สำรองไว้ ลงไปยังระบบสำรองตามความจำเป็นแล้วแต่กรณี ● เชื่อมโยงและเปิดใช้ระบบสำรอง ● ทดสอบใช้งานระบบสำรองตามฟังก์ชั่นที่สำคัญ ๆ ● กรณีที่ระบบสำรองมีปัญหา ให้ร่วมกันพิจารณาปัญหา กำหนดแนวทาง และดำเนินการแก้ไขจนกระทั่งแล้วเสร็จ				
การทดสอบใช้ระบบสำรองโดยผู้ใช้งาน					
3.	ทีมกู้คืนบริการ แจ้งให้ผู้ใช้งานดำเนินการทดสอบระบบสำรอง				
4.	ผู้ใช้งาน ยืนยันว่าระบบสามารถทำงานได้ตามปกติหรือไม่ กลับมายัง ทีมกู้คืนบริการ				
5.	กรณีที่ระบบสำรอง**ไม่สามารถทำงานได้ตามปกติ** ทีมกู้คืนบริการ และ/หรือ ผู้ให้บริการภายนอก ร่วมกันพิจารณาปัญหา กำหนดแนวทางและดำเนินการแก้ไขจนกระทั่งแล้วเสร็จ				
การรายงานผลการกู้คืนระบบ					
6.	ทีมกู้คืนบริการ รายงานผลการกู้ระบบโดยใช้ระบบสำรองให้ หัวหน้าทีมกู้คืนระบบ ได้รับทราบ				

งานที่ต้องทำ		อ้างอิงขั้นตอนปฏิบัติ	ระยะเวลาที่ใช้ในการดำเนินการ	ระยะเวลาที่ทำได้จริง	ลายมือชื่อของผู้ดำเนินการ
7.	หัวหน้าทีมกู้คืนระบบ รายงานผลการแก้ไข ระบบให้คณะกรรมการบริหาร เพื่อรายงาน คณะกรรมการ ให้รับทราบต่อไป				
การสำรองข้อมูลบนระบบสำรอง					
8.	ในระหว่างที่ยังใช้งานระบบสำรองเพื่อ ปฏิบัติงาน ทีมกู้คืนบริการ ดำเนินการสำรอง ข้อมูลบนระบบสำรองด้วยความถี่เดียวกับ ความถี่ในการสำรองข้อมูลของระบบหลัก				

ตารางที่ 1-7 Checklist ของการกู้คืนบริการระบบสารสนเทศ

การทดสอบแผน (Testing & Simulation)

แผนความเสี่ยงและความต่อเนื่องทางธุรกิจด้านเทคโนโลยีสารสนเทศ (Business Continuity Plan: BCP) มีเป้าหมายเพื่อฟื้นฟูระบบให้กลับมาทำงานได้ภายในระยะเวลาที่กำหนด (Recovery Time Objective: RTO) และรักษาความถูกต้องของข้อมูลในระดับที่ยอมรับได้ (Recovery Point Objective: RPO)

การทดสอบแผน BCP เป็นกระบวนการที่มีความสำคัญเชิงกลยุทธ์ เพื่อประเมินความพร้อมของระบบ บุคลากร และกระบวนการที่เกี่ยวข้อง โดยผลการทดสอบจะสะท้อนถึงความสามารถขององค์กรในการตอบสนองต่อเหตุการณ์ฉุกเฉิน และเป็นข้อมูลประกอบการตัดสินใจในการปรับปรุงแผนงานด้าน IT Governance และ Business Continuity Management (BCM)

แบบฟอร์มแผนการทดสอบแผนความเสี่ยงและความต่อเนื่องทางธุรกิจด้านเทคโนโลยีสารสนเทศ (BCP)

วัตถุประสงค์การทดสอบ	ขอบเขตการทดสอบ	ทรัพยากรและเอกสาร	วิธีการทดสอบ	ประเมินผลและจัดทำรายงาน	ฝึกอบรมและรายงานผล
☐เพื่อประเมินความพร้อมของระบบในการรับมือกับเหตุการณ์ภัยพิบัติ	● ระบบสารสนเทศหลัก เช่น ระบบฐานข้อมูล,	● แผน BCP ● รายชื่อผู้รับผิดชอบ	● ปฏิบัติตามแผนที่กำหนด ● บันทึกเวลาในการกู้คืน (Recovery	● วิเคราะห์ผลการทดสอบ	● จัดอบรมให้บุคลากรเข้าใจแผน BCP

☐เพื่อทดสอบความถูกต้องของแผน BCP และความเข้าใจของทีมงาน	ระบบเครือข่าย, ระบบจัดการผู้ใช้ ● บุคลากรที่เกี่ยวข้อง เช่น IT, ผู้บริหาร, ผู้ใช้งาน	● เครื่องมือและระบบสำรอง	Time Objective - RTO) ตามตาราง 1-7 Checklist ของการกู้คืนบริการระบบสารสนเทศ ● ตรวจสอบความสมบูรณ์ของข้อมูล (Recovery Point Objective - RPO)	● ระบุจุดอ่อนและข้อเสนอแนะ ● ปรับปรุงแผน BCP ตามผลการทดสอบ	● รายงานผลการทดสอบกับผู้บริหาร

ตารางที่ 1-8 แบบฟอร์มแผนการทดสอบแผนความเสี่ยงและความต่อเนื่องทางธุรกิจด้านเทคโนโลยีสารสนเทศ

การเฝ้าระวัง ติดตามการดำเนินงาน และการรายงานผล

เมื่อแผน BCP ได้เริ่มต้นดำเนินการแล้ว หัวหน้าทีมกู้คืนระบบ จำเป็นต้องมีการเฝ้าระวังและติดตามการดำเนินงานต่าง ๆ ของลูกทีม แจ้งความคืบหน้าให้หน่วยติดตามสถานการณ์รับทราบเพื่อรายงานต่อ ผู้บัญชาการสูงสุด ต่อไป ตลอดจนสื่อสารไปยังผู้ที่เกี่ยวข้องในทุกระดับตามความจำเป็น

กิจกรรมการดำเนินการที่สำคัญ ๆ ที่เกี่ยวข้องกับการใช้แผน BCP ควรมีการบันทึกเป็นข้อมูลไว้ เพื่อประโยชน์ในการทบทวน และปรับปรุงการดำเนินการเหล่านั้นให้ดียิ่งขึ้นต่อไป ให้ใช้แบบฟอร์มใน ภาคผนวก B เพื่อบันทึกกิจกรรมการดำเนินการที่สำคัญ ๆ เหล่านั้นไว้

ขั้นตอนปฏิบัติสำหรับการสื่อสารไปยังผู้ที่เกี่ยวข้อง

การสื่อสารไปยังผู้ที่เกี่ยวข้องในทุกระดับมี ความสำคัญอย่างยิ่งยวดต่อการใช้แผน BCP นี้ ทั้งนี้เพื่อให้ผู้ที่เกี่ยวข้องได้รับทราบถึงการอัพเดตของ สถานการณ์ที่เกี่ยวข้องกับการกู้คืนบริการ วิธีการสื่อสาร ที่เป็นพื้นฐานในช่วงที่เหตุการณ์หยุดชะงักกำลังดำเนินไป ดังนี้

แผนการแจ้งข้อมูลข่าวสาร

1. ช่องทางการสื่อสาร
    - โทรศัพท์ (ทั้งโทรศัพท์ธรรมดา และโทรศัพท์มือถือ)
    - อีเมล
    - Line
    - SMS

โดยจะเริ่มต้นใช้วิธีการสื่อสารเรียงตามลำดับในข้างต้นจากบนลงมาล่าง กรณีที่ใช้วิธีการในลำดับแรกๆไม่ได้ จะเลื่อนลำดับลงมายังวิธีการในลำดับถัดไป

2. แนวทางในการสื่อสาร ต้องปฏิบัติตามในทุกครั้งที่มีการสื่อสารไปยังผู้ที่เกี่ยวข้อง

- อยู่ในอาการที่สงบเมื่อทำการสื่อสารไปยังผู้ที่เกี่ยวข้อง
- หลีกเลี่ยงการสนทนาที่ยาวนานโดยไม่จำเป็น
- กรณีที่ติดต่อบุคคลตามที่กำหนดไว้ไม่ได้ ให้ดำเนินการดังนี้
    - กรณีมีผู้รับสายแทนให้สอบถามว่ามีข้อมูลติดต่ออื่นของบุคคลตามที่ต้องการ หรือไม่
    - ทิ้งข้อความไว้เพื่อให้ติดต่อกลับตามเบอร์โทรที่ให้ไว้
    - กรณีมีผู้รับสายแทน ไม่ให้รายละเอียดของเหตุการณ์หยุดชะงักที่เกิดขึ้น
- บันทึกข้อมูลที่เกี่ยวข้องกับการติดต่อนั้น ได้แก่ เวลาที่ทำการติดต่อ ได้รับการตอบกลับหรือไม่ และสิ่งที่ได้ดำเนินการจากการติดต่อนั้น ข้อมูลที่ได้มีการสื่อสารกันควรจะมีการบันทึกไว้อย่างถูกต้องและชัดเจนโดยใช้แบบฟอร์มใน ภาคผนวก C ของเอกสารฉบับนี้

3. การสื่อสารภายในองค์กร

กรณีมีความจำเป็นต้องติดต่อบุคลากรหรือหน่วยงาน ภายในต่าง ๆ ให้ดูข้อมูลสำหรับการติดต่อได้ใน ภาคผนวก D

4. การสื่อสารภายนอกองค์กร

หน่วยงานภายนอกที่ทีมกู้คืนบริการจำเป็นต้อง ติดต่อสื่อสารด้วย ได้แก่ ลูกค้า ผู้ให้บริการภายนอก คู่ค้า อื่นๆ โดยดูข้อมูลติดต่อสำหรับหน่วยงานเหล่านี้ใน ภาคผนวก E

ฝึกอบรมบุคลากร (Training)

<u>วิธีปฏิบัติการดำเนินการในระหว่างที่เหตุการณ์เกิดขึ้นแล้ว (During-incident)</u>

สรุปขั้นตอนการดำเนินการในระหว่างที่เหตุการณ์เกิดขึ้นแล้ว ประกอบด้วยขั้นตอนหลักดังนี้

- ☐ รับแจ้ง บันทึก และประสานงานไปยังทีม
- ☐ ประเมินซ้ำ
- ☐ ระดมทีม
- ☐ ประชุมทีม
- ☐ ประกาศเหตุฉุกเฉิน

☐ รับมือหรือจัดการกับเหตุ (ตามแต่กรณี)

☐ ติดตามสถานการณ์และรายงานความคืบหน้า

☐ ตัดสินในดำเนินการต่าง ๆ

โดยมีรายละเอียดในแต่ละขั้นดังนี้

1. รับแจ้ง บันทึกและประสานงานไปยังทีม เมื่อมีเหตุการณ์ความมั่นคงปลอดภัยเกิดขึ้นและมีการรายงานเข้ามา ให้~~หน่วยงานรับแจ้งเหตุสอบถาม~~ ทีมประชาสัมพันธ์รับแจ้งเหตุสอบถาม เพื่อรวบรวมข้อมูลอย่างน้อยดังนี้

- เหตุการณ์ที่เกิด
- ชื่อผู้แจ้งเหตุ
- หน่วยงานของผู้แจ้งเหตุ
- เบอร์โทรศัพท์ติดต่อกลับ
- วัน/เวลาที่พบ
- สถานที่ที่พบเหตุ
- รายละเอียดของเหตุการณ์ เช่น ความเสียหายที่เกิดขึ้น

กรณีเป็นการรายงานเหตุการณ์ฉุกเฉิน ให้ รีบประสานงานแจ้งให้ทีมกู้คืนบริการ ได้รับทราบโดยทันที เพื่อจะได้ประเมินต่อว่าสถานการณ์ที่เกิดขึ้นมีผลกระทบต่อ กระบวนการสำคัญของสถาบันพระบรมราชชนก ดังนี้

- ประเมินว่าเป็นเหตุการณ์ระดับใด
- ประมาณระยะเวลาในการแก้ไข (Projected time to resolve)
- กรณีเป็นเหตุการณ์ระดับ 2 หรือ 3 ทีมกู้คืนบริการ รีบดำเนินการแจ้งให้ผู้บัญชาการสูงสุดและทีมประชาสัมพันธ์ ได้รับทราบโดยเร็วที่สุด(ปฏิบัติตามแผนการแจ้งข้อมูลข่าวสารผ่าน ระบบ Line/Email/โทรศัพท์)

2.ประเมินซ้ำ

- ผู้บัญชาการสูงสุด และทีมรับแจ้งเหตุการณ์หยุดชะงัก ร่วมกันตรวจสอบข้อเท็จจริงอีกครั้ง เพื่อประเมินสถานการณ์อีกครั้งว่าอยู่ในระดับ ความรุนแรงระดับใด มีผลกระทบต่อกระบวนการสำคัญหรือไม่ รวมทั้งใช้ระยะเวลา โดยประมาณเท่าไร ในการแก้ไข (ปฏิบัติตามแนวทางการประเมินซ้ำและทบทวน ข้อมูล)
- หากสามารถควบคุมสถานการณ์ได้ เช่น เป็นเหตุการณ์ระดับ 1 ให้ดำเนินการแก้ไข ตามความจำเป็น และปิดเหตุการณ์ดังกล่าว

3.ระดมทีม หากไม่สามารถควบคุมสถานการณ์ได้ เป็นเหตุการณ์ระดับ 2 หรือ 3

ผู้บัญชาการสูงสุด สั่งการให้ทีมกู้คืนบริการทั้งหมดให้เข้าร่วมปฏิบัติการ (ปฏิบัติตามแผนการแจ้งข้อมูลข่าวสารผ่านระบบ Line/Email/โทรศัพท์)

4.ประชุมทีม

- หากมีเวลาเพียงพอหรือเอื้ออำนวยที่จะประชุมก่อนปฏิบัติการ หัวหน้าทีมกู้คืนระบบสั่งการให้กำหนดสถานที่ประชุม (หรือศูนย์บัญชาการ) และ ประสานงานติดต่อทุกคนที่ได้รับแจ้งในข้างต้น เพื่อขอให้มาประชุมเพื่อประเมิน สถานการณ์ที่เกิดขึ้นร่วมกัน
- ประชุมทีมเพื่อหารือการดำเนินการต่าง ๆ ที่จำเป็น
- มอบหมายให้ทีมลงมือปฏิบัติ

5.ประกาศเหตุฉุกเฉิน

- ผู้บัญชาการสูงสุดหารือร่วมกันและพิจารณาสถานการณ์ที่ เกิดขึ้นร่วมกันว่า เห็นสมควรที่จะประกาศเป็นเหตุฉุกเฉินหรือไม่
- กรณีที่เห็นสมควร ดำเนินการประกาศเป็นเหตุฉุกเฉินเพื่อให้บุคลากร ผู้ใช้บริการ หน่วยงานภายนอก ประชาชน หรือผู้เกี่ยวข้องอื่น ๆ ได้รับทราบ (ปฏิบัติ ตามแผนการแจ้งข้อมูลข่าวสารผ่านระบบ Line/Email/โทรศัพท์)

6.รับมือหรือจัดการกับเหตุ (ตามแต่กรณี)

ใช้แผนความเสี่ยงและความต่อเนื่องทางธุรกิจด้านเทคโนโลยีสารสนเทศ (Business Continuity Plan : BCP) จัดการตามแต่กรณีของเหตุการณ์

7.ติดตามสถานการณ์และรายงานความคืบหน้า

-หน่วยติดตามสถานการณ์ คอยติดตามสถานการณ์และความคืบหน้าอย่างต่อเนื่อง และรายงานให้ผู้บัญชาการสูงสุด ได้รับทราบเพื่อเป็นข้อมูลในการตัดสินใจหรือสั่งการเพิ่มเติมตามสมควร

- ทีมประชาสัมพันธ์ แจ้งความคืบหน้าในการดำเนินการให้พนักงานและผู้ที่ เกี่ยวข้องได้รับทราบ (ปฏิบัติตามแผนการแจ้งข้อมูลข่าวสารผ่านระบบ Line/Email/ โทรศัพท์)

8.ตัดสินในดำเนินการต่าง ๆ

- ผู้บัญชาการสูงสุด ตัดสินใจดำเนินการต่าง ๆ ตามข้อมูล ที่ได้รับ
- กรณีพบว่ากระบวนการสำคัญหรือระบบสนับสนุน เกิดการหยุดชะงัก และเป็นเหตุการณ์ระดับ 2 หรือ 3 ผู้บัญชาการสูงสุด สั่งการหัวหน้าทีมกู้คืนระบบ นำแผน BCP มาใช้งาน

<u>วิธีปฏิบัติการดำเนินการเมื่อเกิดเหตุการณ์ยุติลงแล้ว (After-incident) และการประเมินสัมฤทธิ์ผลของการดำเนินการทั้งหมด (Effectiveness Evaluation)</u>

การยกเลิกเหตุฉุกเฉิน เมื่อสถานการณ์ที่ได้รับรายงานเข้ามา เข้าสู่สภาวะปกติแล้วให้ผู้บัญชาการสูงสุด สั่งการให้สิ้นสุดปฏิบัติการ โดย

1.ประกาศการกลับคืนสู่สภาวะปกติให้ทั้งพนักงานและผู้ที่เกี่ยวข้องภายในและภายนอกสถาบัน ได้รับทราบ “ประกาศยกเลิกภาวะฉุกเฉิน” รวมทั้งสร้างขวัญและกำลังใจของบุคลากร ให้กลับคืนมา

2.ประกาศแจ้งสถานภาพความพร้อมใช้ระบบเทคโนโลยีสารสนเทศ หรืออื่น ๆ ที่ เกี่ยวข้อง

3.ทีมประชาสัมพันธ์ ประกาศแจ้งให้พนักงานและผู้ที่เกี่ยวข้องได้รับทราบ(ปฏิบัติตามแผนการแจ้งข้อมูลข่าวสารผ่านระบบ Line/Email/โทรศัพท์)

4.การประเมินความสัมฤทธิ์ผลของการดำเนินการทั้งหมด (Effectiveness Evaluation)

1.ทีมกู้คืนบริการ ทำสำเนา 1 ชุดของข้อมูลที่ได้บันทึกไว้ระหว่างปฏิบัติการ เช่น รายงาน ข้อความ หรือเอกสารอื่น ๆ และส่งมอบสำเนาให้กับ
ผู้บัญชาการสูงสุด รวมทั้งจัดเก็บต้นฉบับไว้อย่างน้อย 1 ปี

2.ผู้บัญชาการสูงสุด สั่งการให้ทุกหน่วยจัดทำรายงาน
After Action Report เพื่อทบทวนตามรายการข้างล่างนี้

1)การเตรียมการก่อนการเกิดเหตุการณ์ความมั่นคงปลอดภัยไซเบอร์

2)การจัดการกับเหตุการณ์ฯที่ได้ดำเนินไปทั้งหมด เพื่อดูว่ามีความเหมาะสมหรือไม่ หรือต้องปรับปรุงอย่างไร

รายงาน ควรมีเนื้อหาครอบคลุมในประเด็น ดังนี้

- ระบุสาเหตุของเหตุการณ์ที่เกิดขึ้น
- ประเมินค่าความเสียหายที่เกิดขึ้น
- ประเมินผลกระทบที่มีต่อชื่อเสียงและภาพลักษณ์ของสถาบันพระบรมราชชนก
- ระบุการดำเนินการแก้ไข เพื่อป้องกันการเกิดขึ้นซ้ำอีกของเหตุการณ์นี้ในอนาคต
- ประเมินความเหมาะสมในการตัดสินใจดำเนินการ เพื่อรับมือและจัดการกับเหตุที่เกิดขึ้น
- ประเมินความเหมาะสมด้านระยะเวลาที่ใช้ในการแก้ไขกระบวนการสำคัญและระบบ สำคัญเพื่อให้กลับคืนมาให้บริการได้
- ประเมินความเหมาะสมด้านสิ่งต่าง ๆ ที่ได้เตรียมการไว้ก่อนล่วงหน้า
- ทบทวนจากข้อมูลที่บันทึกไว้ระหว่างการเกิดเหตุ ว่ามีสิ่งใดที่มองข้ามไป คาดการณ์ผิด หรือเป็นข้อบกพร่องที่ต้องแก้ไข
- พิจารณาว่าแผนการบริหารจัดการกับเหตุการณ์ความมั่นคงปลอดภัยนี้ ควรปรับปรุง ให้ครอบคลุมในจุดไหนมากขึ้น หรือเพื่อให้ใช้งานหรือรับมือในสถานการณ์ได้ดีขึ้น
- พิจารณาว่าจำเป็นต้องมีการอบรม ฝึกฝน หรือสร้างความตระหนักเพิ่มเติมหรือไม่

- ระบุสิ่งที่ต้องดำเนินการปรับปรุงหรือแก้ไขเพิ่มเติม เช่น นโยบาย ขั้นตอนการปฏิบัติ หรืออื่น ๆ

3.ทุกหน่วย ส่งมอบรายงาน After Action Report ให้ผู้บัญชาการสูงสุด และผู้บริหารระดับสูงต่อไป เพื่อพิจารณาและให้คำแนะนำหรือตอบกลับต่อรายงานดังกล่าว เพื่อนำไปสู่การ ปรับปรุงการบริหารจัดการเหตุการณ์ความมั่นคงปลอดภัยให้ดียิ่งขึ้นต่อไป

การฟื้นฟู ได้แก่ การนำรายงานผลการประเมินผลมาปรับปรุงแก้ไข โดยเฉพาะ BCM และ BMP/DRP รวมถึงการปรับปรุงบุคลากรที่ปฏิบัติหน้าที่

การทบทวน ให้บริหารกำหนดให้มีการทบทวนแผน อย่างน้อยปีละหนึ่งครั้ง