คู่มือการจัดทำแผนเตรียมความพร้อม
กรณีเกิดเหตุฉุกเฉินด้านสารสนเทศ ทร.

สารบัญ

หลักการและเหตุผล ๑

กฎหมาย ระเบียบ ที่เกี่ยวข้อง ๑

วัตถุประสงค์ของการจัดทำแผนเตรียมความพร้อมกรณีเกิดเหตุฉุกเฉินด้านสารสนเทศ ทร. ๑

แนวทางการเตรียมความพร้อมของหน่วยงานต่อเหตุฉุกเฉินด้านสารสนเทศ ๒

การจัดทำแผนเตรียมความพร้อมกรณีเกิดเหตุฉุกเฉินด้านสารสนเทศ ๓

๑. การกำหนดโครงสร้างและทีมงานรับผิดชอบแผนเตรียมความพร้อมกรณีเกิดเหตุฉุกเฉินด้านสารสนเทศ ๓

๒. การบริหารจัดการความเสี่ยงภัยคุกคาม/ ๔

๒๑. การวิเคราะห์ความเสี่ยง ๔

๒๒. การประมาณความเสี่ยง ๖

๒๓. มาตรการจัดการความเสี่ยง ๖

๓. จัดทำมาตรการรองรับแต่ละความเสี่ยง ๗

สรุป ๘

ผนวก ตัวอย่าง แผนเตรียมความพร้อมกรณีเกิดเหตุฉุกเฉินด้านสารสนเทศ ศูนย์ข้อมูลกลาง สำนักปฏิบัติการ กรมการสื่อสารและเทคโนโลยีสารสนเทศทหารเรือ

คู่มือการจัดทำแผนเตรียมความพร้อมกรณีเกิดเหตุฉุกเฉินด้านสารสนเทศ ทร.

หลักการและเหตุผล

ปัจจุบัน ทร. ได้นำเอาระบบสารสนเทศเข้ามาใช้งานภายในหน่วยงานทุก นขต.ทร. เพื่อเป็นการลดโอกาสความเสียหายที่เกิดขึ้นจากเหตุการณ์ไม่พึงประสงค์ รวมทั้งจากสถานการณ์ฉุกเฉินต่าง ๆ การจัดทำแผนเตรียมความพร้อมกรณีเกิดเหตุฉุกเฉินด้านสารสนเทศ จึงเป็นการเตรียมการรับมือกับเหตุการณ์ฉุกเฉินในรูปแบบต่าง ๆ เพื่อให้หน่วยสามารถดำเนินภารกิจได้ในสภาวะวิกฤตได้อย่างมีประสิทธิภาพ ดังนั้น สสท.ทร. จึงมีการดำเนินการกำหนดแนวทางในการจัดทำแผนเตรียมความพร้อมกรณีเกิดเหตุฉุกเฉินด้านสารสนเทศ ทร. ขึ้นเพื่อเป็นแนวทางให้หน่วยต่าง ๆ ของ ทร. ที่มีระบบเครือข่ายคอมพิวเตอร์และระบบสารสนเทศได้ดำเนินการจัดทำแผนเตรียมความพร้อมกรณีเกิดเหตุฉุกเฉินด้านสารสนเทศสำหรับใช้ภายในหน่วย อันจะช่วยทำให้ทุกหน่วยงานของ ทร. มีความรู้ความเข้าใจในแนวทางบริหารจัดการหน่วยงานเพื่อเตรียมความพร้อมต่อสภาวะวิกฤต และทำให้สามารถใช้งานระบบสารสนเทศและเครือข่ายได้อย่างต่อเนื่องเป็นระบบ และมีประสิทธิภาพ โดยคู่มือนี้ประกอบไปด้วย ๒ ส่วน คือ <u>ส่วนแรก</u> เป็นแนวทางจัดทำแผนเตรียมความพร้อมกรณีเกิดเหตุฉุกเฉินด้านสารสนเทศ ทร. ซึ่งสอดคล้องกับมาตรฐานสากล BS2599 Business Continuity Management และ <u>ส่วนที่สอง</u> (ภาคผนวก) เป็นตัวอย่างในการพัฒนาแผนเตรียมความพร้อมกรณีเกิดเหตุฉุกเฉินด้านสารสนเทศของ ศูนย์ข้อมูลกลาง (ศขก.) สปก.สสท.ทร.

กฎหมาย ระเบียบ ที่เกี่ยวข้อง

๑. ระเบียบสำนักนายกรัฐมนตรีว่าด้วยการรักษาความลับทางราชการ พ.ศ.๒๕๔๔
๒. ระเบียบสำนักนายกรัฐมนตรีว่าด้วยการรักษาความปลอดภัยแห่งชาติ พ.ศ.๒๕๕๒
๓. พ.ร.บ.ว่าด้วยกระการทำผิดทางคอมพิวเตอร์ พ.ศ.๒๕๕๐
๔. ระเบียบ ทร. ว่าด้วยการรักษาความปลอดภัยระบบสารสนเทศ พ.ศ.๒๕๕๔
๕. นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของกองทัพเรือ พ.ศ.๒๕๕๘
๖. แนวทางการใช้งานระบบสารสนเทศของกองทัพเรือ พ.ศ.๒๕๕๘

วัตถุประสงค์ของการจัดทำแผนเตรียมความพร้อมกรณีเกิดเหตุฉุกเฉินด้านสารสนเทศ ทร.

๑. เพื่อให้หน่วยสามารถใช้เป็นแนวทางในการเตรียมความพร้อมและรองรับสถานการณ์ฉุกเฉิน ที่อาจจะเกิดขึ้นและมีผลกระทบต่อระบบเทคโนโลยีสารสนเทศและเครือข่าย รวมถึงการสื่อสารของหน่วยงาน

๒. เพื่อให้หน่วยสามารถสามารถวางแผนควบคุมและแก้ไขความเสี่ยงด้านเทคโนโลยีสารสนเทศ

๓. เพื่อนำกรณีศึกษาในการจัดทำแผนเตรียมความพร้อมกรณีเกิดเหตุฉุกเฉินให้กับเจ้าหน้าที่ที่เกี่ยวข้องนำไปปฏิบัติ

๔. เพื่อช่วยเพิ่มประสิทธิภาพการตัดสินใจ โดยคำนึงถึงปัจจัยเสี่ยงด้านต่าง ๆ ที่จะมีผลกระทบกับการดำเนินงาน แล้วพิจารณาหาแนวทางในการป้องกันหรือจัดการปัจจัยเสี่ยง ก่อนเริ่มปฏิบัติงานหรือดำเนินงานตามแผน

แนวทางการเตรียมความพร้อมของหน่วยงานต่อเหตุฉุกเฉินด้านสารสนเทศ

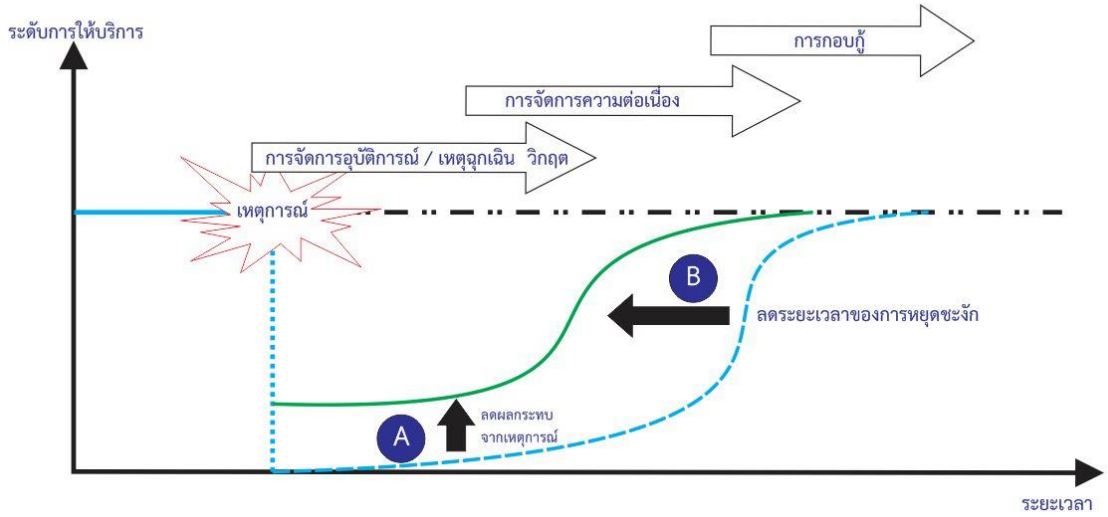
สำหรับแนวคิดการเตรียมความพร้อมต่อเหตุฉุกเฉินด้านสารสนเทศของ ทร. หน่วยงานต่าง ๆ ภายใน ทร. ควรเน้นควบคุมดูแลและป้องกันทรัพยากรด้านสารสนเทศที่สำคัญต่อการดำเนินงานหรือให้บริการ เพื่อสร้างประโยชน์สูงสุดสำหรับผู้รับบริการ (ข้าราชการภายในหรือภายนอกหน่วยงาน) โดยหากการควบคุมภายในที่มีอยู่ไม่สามารถควบคุมดูแลและป้องกันได้ทั้งหมดเมื่อเกิดสถานการณ์ฉุกเฉินขึ้น ระดับการดำเนินงานหรือให้บริการของหน่วยงานจะลดลง ดังนั้นบทบาทหน้าที่ของหน่วยงานคือต้องรีบดำเนินการให้ระดับการดำเนินงานหรือให้บริการกลับมาในระดับที่เหมือนภาวะปกติให้เร็วที่สุด ซึ่งอาจแยกได้เป็น

๑. ภายในช่วงระยะเวลาแรก จะเป็นช่วงของการตอบสนองต่อสถานการณ์ (Incident/ Emergency Management) ในกรณีที่เหตุการณ์และความเสียหายขยายตัวไปในวงกว้าง การตอบสนองอาจจำเป็นต้องยกระดับเป็นการบริหารจัดการวิกฤต (Crisis Management)

๒. ภายหลังจากนั้น จะเป็นช่วงของการทำให้เกิดความต่อเนื่องของกระบวนการทำงานของระบบ (Continuity Management) เพื่อให้หน่วยงานสามารถกลับมาดำเนินงานได้ ซึ่งแยกเป็น ๒ ระดับ

๒.๑ ดำเนินงานหรือให้บริการได้ในระดับที่องค์กรยอมรับกับผลกระทบที่เกิดขึ้นกับผู้รับบริการและผู้มีส่วนได้ส่วนเสียทั้งหมดภายในระยะเวลาอันสั้น

๒.๒ กลับมาให้บริการได้ในระดับปกติตามระยะเวลาที่กำหนด ในช่วงการดำเนินการกอบกู้กระบวนการทำงานของระบบ (Recovery) ดังแสดงตามรูปที่ ๑



รูปที่ ๑ แนวคิดการบริหารความต่อเนื่อง

ที่มา ISO/PAS 22399-2007 Social Security –Guideline for incident preparedness and operational Continuity management

สภาวะวิกฤตหรือเหตุการณ์ฉุกเฉินต่าง ๆ หากเกิดขึ้นอาจส่งผลกระทบให้ระบบสารสนเทศของหน่วยงานไม่สามารถดำเนินงานหรือให้บริการได้ตามปกติ ดังนั้น จึงมีความจำเป็นที่หน่วยงานต้องจัดทำแผนเตรียมความพร้อมกรณีเกิดเหตุฉุกเฉินด้านสารสนเทศ เพื่อเตรียมพร้อมรับภัยคุกคามที่อาจเกิดขึ้นกับระบบสารสนเทศ โดยวัตถุประสงค์ ของการจัดทำแผนเตรียมความพร้อมมีดังนี้

๑. เพื่อใช้เป็นแนวทางให้หน่วยสามารถบริหารความต่อเนื่องของการใช้งานหรือการให้บริการระบบสารสนเทศได้ในสภาวะวิกฤต

๒. เพื่อให้หน่วยงานมีการเตรียมความพร้อมล่วงหน้าในการรับมือกับสภาวะวิกฤตหรือเหตุการณ์ฉุกเฉินต่าง ๆ ที่อาจเกิดขึ้น

๓. เพื่อลดผลกระทบจากการหยุดชะงักในการดำเนินงาน เช่น ผลกระทบด้านเศรษฐกิจการเงิน การให้บริการ สังคม ชุมชน และสิ่งแวดล้อม ตลอดจนชีวิตและทรัพย์สินของประชาชน เป็นต้น

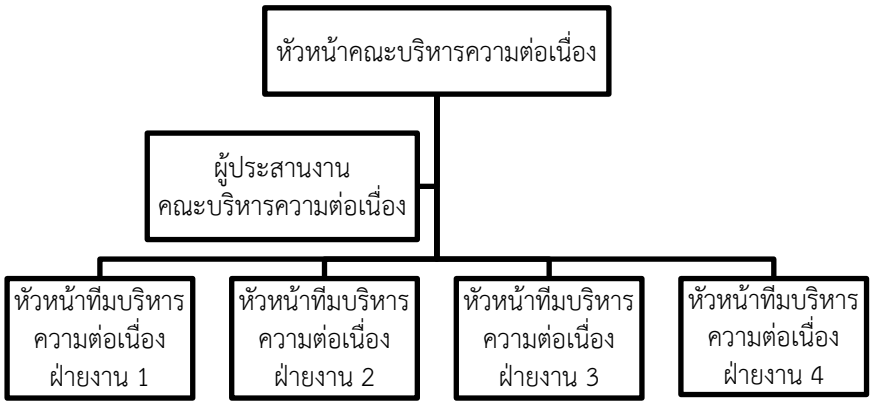
๔. เพื่อบรรเทาความเสียหายให้อยู่ในระดับที่ยอมรับได้

การจัดทำแผนเตรียมความพร้อมกรณีเกิดเหตุฉุกเฉินด้านสารสนเทศ

คู่มือฉบับนี้จะนำเสนอแนวทางในการจัดทำแผนเตรียมความพร้อมกรณีเกิดเหตุฉุกเฉินด้านสารสนเทศ เพื่อให้หน่วยงานของ ทร. นำไปปรับใช้ให้เหมาะสมและสอดคล้องกับการดำเนินงานและการให้บริการระบบสารสนเทศของหน่วยงาน เพื่อให้ระบบสารสนเทศของหน่วยงาน สามารถให้บริการได้อย่างต่อเนื่อง และเจ้าหน้าที่ผู้ดูแลระบบสารสนเทศนั้น ๆ มีแนวทางในการจัดการกับเหตุฉุกเฉินด้านสารสนเทศต่าง ๆ ที่อาจจะเกิดขึ้นได้ โดยการจัดทำแผนเตรียมความพร้อมกรณีเกิดเหตุฉุกเฉินด้านสารสนเทศนี้ แบ่งโครงสร้างที่สำคัญออกเป็น ๓ ขั้นตอนหลัก ดังนี้

๑. การกำหนดโครงสร้างและทีมงานรับผิดชอบแผนเตรียมความพร้อมกรณีเกิดเหตุฉุกเฉินด้านสารสนเทศ

เพื่อให้การจัดทำและการปฏิบัติตามแผนเตรียมความพร้อมกรณีเกิดเหตุฉุกเฉินด้านสารสนเทศเป็นไปอย่างมีประสิทธิภาพ ชัดเจนในสายการบังคับบัญชาและการควบคุม และไม่เกิดความสับสนในการปฏิบัติ การจัดตั้งทีมงานรับผิดชอบแผนฯ ของหน่วยงาน จึงเป็นขั้นตอนแรกที่ต้องมีการพิจารณากำหนดขึ้น โดยนำเจ้าหน้าที่ผู้ที่มีส่วนเกี่ยวข้องหลักของระบบสารสนเทศต่าง ๆ เข้ามาอยู่ในทีมงาน โดยอาจมีโครงสร้าง ดังนี้



บุคลากรหลัก		บทบาท	บุคลากรสำรอง	
ชื่อ	หมายเลขโทรศัพท์		ชื่อ	หมายเลขโทรศัพท์
xxxxxxxxxx	๐๘x xxxx xxx	หัวหน้าคณะบริหารแผนฯ	xxxxxxxxxx	๐๘x xxxx xxx
xxxxxxxxxx	๐๘x xxxx xxx	ผู้ประสานงานคณะบริหารแผนฯ	xxxxxxxxxx	๐๘x xxxx xxx
xxxxxxxxxx	๐๘x xxxx xxx	หัวหน้าทีมบริหารแผนฯ ฝ่ายงาน ๑	xxxxxxxxxx	๐๘x xxxx xxx
xxxxxxxxxx	๐๘x xxxx xxx	หัวหน้าทีมบริหารแผนฯ ฝ่ายงาน ๒	xxxxxxxxxx	๐๘x xxxx xxx

บุคลากรหลัก		บทบาท	บุคลากรสำรอง	
ชื่อ	หมายเลขโทรศัพท์		ชื่อ	หมายเลขโทรศัพท์
xxxxxxxxxx	๐๘x xxxx xxx	หัวหน้าทีมบริหารแผนฯ ฝ่ายงาน ๓	xxxxxxxxxx	๐๘x xxxx xxx
xxxxxxxxxx	๐๘x xxxx xxx	หัวหน้าทีมบริหารแผนฯ ฝ่ายงาน ๔	xxxxxxxxxx	๐๘x xxxx xxx

๒. การบริหารจัดการความเสี่ยง/ภัยคุกคาม

ความเสี่ยง หรือภัยคุกคาม หมายถึง เหตุการณ์หรือการกระทำใดๆ ที่อาจจะเกิดขึ้นภายในสถานการณ์ที่ไม่แน่นอน และจะส่งผลกระทบหรือสร้างความหรือก่อให้เกิดความล้มเหลวหรือลดโอกาสที่จะบรรลุวัตถุประสงค์ และเป้าหมายของหน่วยงาน ทั้งในด้านยุทธศาสตร์การปฏิบัติงาน งบประมาณ และการบริการ ซึ่งอาจเป็นผลกระทบทางบวกด้วยก็ได้ โดยวัดจากผลกระทบ (Impact) ที่ได้รับและโอกาสที่จะเกิด (Likelihood) ของเหตุการณ์

การบริหารจัดการความเสี่ยง เป็นกระบวนการที่ใช้ในการบริหารจัดการ ให้โอกาสที่จะเกิดเหตุการณ์ความเสี่ยง/ภัยคุกคามลดลงหรือหมดไป หรือผลกระทบของความเสียหายจากเหตุการณ์ความเสี่ยงลดลงอยู่ในระดับที่หน่วยงานยอมรับได้ ซึ่งการจัดการความเสี่ยงสามารถดำเนินการได้ ๔ แนวทางหลัก คือ การยอมรับความเสี่ยง การหลีกเลี่ยงความเสี่ยง การควบคุมความเสี่ยง และการถ่ายโอนความเสี่ยง โดยขั้นตอนการบริหารจัดการความเสี่ยงประกอบด้วย

๒.๑ การวิเคราะห์ความเสี่ยง ประกอบด้วยกระบวนการย่อย ๓ กระบวนการคือ

- <u>การชี้ระบุความเสี่ยง (Risk Identification)</u> เป็นการชี้ให้เห็นถึงความเสี่ยงที่หน่วยงานเผชิญอยู่ กระบวนการนี้จำเป็นต้องอาศัยความรู้ความเข้าใจหน่วยงาน ภารกิจและกิจกรรม ปัจจัยที่มีผลต่อความสำเร็จของหน่วยงาน รวมถึงโอกาสและภัยคุกคามที่มีต่อหน่วยงาน การชี้ระบุความเสี่ยงควรได้ดำเนินการอย่างครอบคลุมกิจกรรมในทุก ๆ ด้านของหน่วยงาน สาเหตุสำคัญของความเสี่ยงคือ การมีภัยคุกคามที่อาจส่งผลให้เกิดการละเมิดความมั่นคงปลอดภัยทางสารสนเทศ และส่งผลเสียตามมา

การชี้ระบุความเสี่ยง อาจพิจารณาถึงเหตุการณ์หรือสิ่งที่เคยเกิดขึ้นมาแล้วในอดีตกับหน่วยงานนั้นหรือหน่วยงานอื่นใด หรืออาจเป็นสิ่งที่มีความเป็นไปได้ว่าจะเกิดขึ้นแม้ไม่เคยเกิดขึ้นมาก่อนก็ได้ กระบวนการ ในการชี้ระบุความเสี่ยงอาจจะใช้วิธีการต่าง ๆ ร่วมกันดังนี้ เช่น

- การระดมสมอง
- การออกแบบสอบถาม
- การวิเคราะห์กระบวนการทำงานหรือกิจกรรมในภารกิจ
- การวิเคราะห์สภาพการณ์เหตุการณ์ละเมิดความมั่นคง
- การประชุมเชิงปฏิบัติการด้านการประเมินความเสี่ยง
- การสืบสวนเหตุการณ์ละเมิดความมั่นคงสารสนเทศ
- การตรวจสอบและตรวจสภาพระบบ
- การวิเคราะห์สถานการณ์

- <u>บรรยายลักษณะรายละเอียดของความเสี่ยง (Description of risk)</u> เมื่อชี้ระบุความเสี่ยงแล้วให้นำมาบรรยายรายละเอียดและลักษณะของความเสี่ยงนั้น ได้แก่

- ชื่อความเสี่ยง
- ขอบเขต
- ลักษณะความเสี่ยง

○ผู้ที่มีผลกระทบ
○ลักษณะเชิงประมาณ
○การยอมรับความเสี่ยง
○การบำบัดและการควบคุม
○แนวทางการปรับปรุง
○การพัฒนากลยุทธ์และนโยบาย

- การประมาณความเสี่ยง (Risk estimation) ขั้นตอนนี้เป็นการดูปัญหาความเสี่ยงในแง่ของโอกาสการเกิดเหตุ (incident) หรือเหตุการณ์ (event) ว่ามีมากน้อยเพียงไร และผลที่ติดตามมาว่ามีความรุนแรงหรือเสียหายมากน้อยเพียงใด

โอกาสหรือความน่าจะเป็นหรือความบ่อยครั้งของการเกิดเหตุหรือเหตุการณ์ อาจแบ่งง่าย ๆ เป็น ๕ ระดับ จากน้อยไปหามาก เช่น

ระดับโอกาสการเกิดเหตุการณ์ต่าง ๆ		
ระดับ	โอกาสที่จะเกิด	คำอธิบาย
๕	บ่อยมาก	๕ ครั้ง/ปี
๔	เป็นไปได้	๔ ครั้ง/ปี
๓	เกิดขึ้นได้ตามโอกาส	๓ ครั้ง/ปี
๒	เกิดขึ้นได้น้อยครั้งมาก	๒ ครั้ง/ปี
๑	แทบไม่เกิดขึ้นเลย	ไม่เกิน ๑ ครั้ง/ปี

ค่าความเสียหายที่เกิดขึ้นจากเหตุการณ์ เช่น

ระดับความรุนแรงของความเสียหายที่เกิดขึ้นจากเหตุการณ์		
ระดับ	ผลกระทบ	คำอธิบาย
๕	สูงมาก	เกิดความเสียหายต่อระบบสารสนเทศ/ข้อมูลที่สำคัญทั้งหมด
๔	สูง	เกิดปัญหากับระบบสารสนเทศ/ข้อมูลที่สำคัญบางส่วน
๓	ปานกลาง	ระบบมีปัญหาและมีความสูญเสียไม่มาก
๒	ต่ำ	เกิดเหตุร้ายเล็กน้อยที่แก้ไขได้
๑	ต่ำมาก	เกิดเหตุร้ายที่ไม่มีความสำคัญ

จากการวิเคราะห์ความเสี่ยง นอกจากการดำเนินการตามขั้นตอนย่อยทั้ง ๓ ข้างต้นแล้ว เรายังควรแยกประเภทความเสี่ยงออกเป็น ๔ ด้านดังนี้

○ความเสี่ยงด้านเทคนิค เป็นความเสี่ยงที่อาจเกิดขึ้นจากระบบคอมพิวเตอร์ เครื่องมือและอุปกรณ์เองอาจเสียหาย หรือเกิดการโจมตีจากผู้ไม่ประสงค์ดี หรือมัลแวร์ เป็นต้น

○ความเสี่ยงด้านผู้ปฏิบัติงาน เป็นความเสี่ยงที่อาจเกิดขึ้นจากการดำเนินการ การจัดความสำคัญในการเข้าถึงไม่เหมาะสม หรือการพึ่งพาเจ้าหน้าที่ และเจ้าหน้าที่นั้นไม่สามารถปฏิบัติงานตามที่กำหนดในหน้าที่ความรับผิดชอบของตนได้

○ความเสี่ยงทางกายภาพ เป็นความเสี่ยงที่เกิดจากภัยคุกคามทางธรรมชาติและสิ่งแวดล้อมที่มนุษย์กระทำขึ้น ลักษณะทางกายภาพและสิ่งแวดล้อมทั้งโดยเจตนาและไม่เจตนา เช่น ภัยธรรมชาติ กระแสไฟฟ้าขัดข้อง เพลิงไหม้ เป็นต้น

○ความเสี่ยงด้านการบริหารจัดการ เป็นความเสี่ยงจากแนวนโยบายการบริหารจัดการที่อาจส่งผลกระทบต่อการดำเนินการด้านสารสนเทศ

๒.๒ การประมาณความเสี่ยง เป็นขั้นตอนต่อเนื่องจากการวิเคราะห์ความเสี่ยง โดยนำความเสี่ยงที่ระบุได้ มาจัดลำดับความสำคัญ โดยคำนึงถึง โอกาสที่อาจจะเกิดขึ้นได้ และ ค่าความเสียหายหากความเสี่ยงนั้นเกิดขึ้น ซึ่งมีวิธีการประมาณความเสี่ยงดังนี้

ระดับความเสี่ยง = โอกาสในการเกิดเหตุการณ์ x ค่าความเสียหายหากเหตุการณ์นั้นเกิดขึ้น

ผลการประมาณความเสี่ยงสามารถแสดงได้ในแผนภูมิความเสี่ยงดังนี้

๒.๓ มาตรการจัดการความเสี่ยง

เมื่อเราสามารถจัดลำดับความสำคัญของความเสี่ยงได้แล้ว เราสามารถกำหนดมาตรการจัดการความเสี่ยง สอดคล้องกับค่าความสำคัญของความเสี่ยงได้ ทั้งนี้เนื่องจากการกำหนดมาตรการรองรับความเสี่ยงทั้งหมดด้วยบุคลากรในหน่วยงานเอง เป็นเรื่องที่ทำได้ยาก เนื่องจากข้อจำกัดทางด้านทรัพยากรของหน่วยงาน ไม่ว่าจะเป็น งบประมาณ จำนวนบุคลากร และเวลา ที่มีอยู่อย่างจำกัด ดังนั้น เมื่อเราสามารถจัดลำดับความสำคัญของความเสี่ยงได้แล้ว จะเห็นว่า บางเหตุการณ์หากมีโอกาสเกิดขึ้นมาก และเมื่อเกิดแล้วจะมีความเสียหายมาก จำเป็นต้องมีมาตรการรองรับ แต่บางความเสี่ยงมีโอกาสที่จะเกิดขึ้นน้อย และเมื่อเกิดแล้วจะมีความเสียหายต่ำ เราสามารถที่จะยอมรับความเสี่ยงที่จะเกิดนั้นได้ เป็นต้น โดยมาตรการจัดการความเสี่ยงสามารถแบ่งออกได้เป็น ๔ ประเภท ดังนี้

○ การยอมรับความเสี่ยง คือการยอมรับความเสี่ยงในระดับที่อยู่และให้ระบบสารสนเทศสามารถดำเนินงานได้ตามปกติ ซึ่งเป็นการยอมรับในผลที่อาจจะเกิดขึ้นตามมา เช่น การพิสูจน์ตัวตนเพียงใช้ username และ password มีความเสี่ยงเพราะอาจมีการขโมยไปใช้ได้ การใช้มาตรการพิสูจน์ตัวตนอื่นที่ปลอดภัยกว่าอาจมีค่าใช้จ่ายสูงไม่คุ้มค่ากับการลงทุน หน่วยงานอาจยอมรับความเสี่ยงของมาตรการในปัจจุบัน และปรับปรุงให้ดียิ่งขึ้นเมื่อมีโอกาส

○ การหลีกเลี่ยงความเสี่ยง เป็นการกำจัดสาเหตุของความเสี่ยง เช่น เมื่อพบว่าปัจจุบันหน่วยงานมีการสำรองข้อมูลเพียง ๑ ชุด และจัดเป็นความเสี่ยงต่อการสูญเสีย การหลีกเลี่ยงความเสี่ยงอาจได้แก่ การสำรองข้อมูล ๒ ชุดและแยกจัดเก็บในสถานที่ต่างกัน เป็นต้น

- การควบคุมความเสี่ยง คือการทำเพื่อให้โอกาสเกิดผลกระทบต่อระบบสารสนเทศจากเหตุการณ์ความเสี่ยงเกิดน้อยที่สุด และหากเกิดขึ้นก็สามารถจำกัดความเสียหายและทำให้ระบบสารสนเทศกลับเข้าสู่สภาวะปกติให้เร็วที่สุด

- การถ่ายโอนความเสี่ยง คือการหาทางเลือกอื่นเพื่อชดเชยหรือจำกัดความเสียหาย เช่น อุปกรณ์คอมพิวเตอร์เมื่อจัดหามาแล้วมีระยะเวลารับประกัน ๓ ปี หากเกิดความเสียหายในช่วงเวลาดังกล่าว เราสามารถถ่ายโอนความเสียหายที่เกิดขึ้น ให้กับบริษัทคู่สัญญาเป็นผู้รับผิดชอบดำเนินการได้

๓. จัดทำมาตรการรองรับแต่ละความเสี่ยง

หลังจากที่ทราบถึงความเสี่ยงที่มีต่อระบบสารสนเทศทั้งหมด และได้มีการจัดลำดับความสำคัญของความเสี่ยงแล้ว ในขั้นตอนต่อไป จะเป็นการกำหนดมาตรการรองรับแต่ละความเสี่ยง ซึ่งมาตรการดังกล่าวเป็นคู่มือการดำเนินการให้กับเจ้าหน้าที่ที่รับผิดชอบด้านต่าง ๆ ใช้อ้างอิงการปฏิบัติ โดยมาตรการรองรับความเสี่ยงควรมีหัวข้อการดำเนินการอย่างน้อยดังต่อไปนี้

๑. <u>ผู้สั่งการในที่เกิดเหตุ</u> ในแต่ละความเสี่ยงหรือสถานการณ์ฉุกเฉินด้านสารสนเทศนั้น อาจมีผู้เกี่ยวข้องกับการปฏิบัติเพื่อตอบสนองเหตุการณ์นั้น ๆ หลายผู้เกี่ยวข้อง ดังนั้นเพื่อให้ความชัดเจนว่าผู้ใดเป็นผู้รับผิดชอบการปฏิบัติในภาพรวมและไม่เกิดความสับสนในการสั่งการแก้ไขปัญหา จึงควรกำหนดผู้สั่งการในที่เกิดเหตุให้ชัดเจน เพื่อสามารถกำหนดการดำเนินการได้อย่างเป็นเอกภาพ และเกิดความชัดเจนในการควบคุมบังคับบัญชาการแก้ไขปัญหาที่เกิดขึ้น

๒. <u>การตรวจสอบและสรุปหาสาเหตุเบื้องต้น</u> การจะเลือกมาตรการรองรับความเสี่ยงที่ถูกต้องมาใช้กับสถานการณ์ฉุกเฉินที่เกิดขึ้นนั้น จะต้องทราบถึงสาเหตุหรือที่มาของความเสียหาย หรือสถานการณ์ฉุกเฉินเสียก่อน ซึ่งในขั้นตอนนี้จะระบุถึงที่มาของสถานการฉุกเฉินที่เกิดขึ้น รวมถึงขั้นตอนในการตรวจสอบอุปกรณ์ หรือระบบที่เกี่ยวข้อง เพื่อให้ทราบถึงขอบเขตของความเสียหาย รวมถึงทราบว่าผู้เกี่ยวข้องที่จะต้องรับผิดชอบดำเนินการจัดการกับสถานการณ์ฉุกเฉินดังกล่าว มีใครบ้าง

๓. <u>การรายงานเหตุ</u> ตามหลักการแล้วทุกครั้งที่เกิดสถานการณ์ฉุกเฉินหรือความเสียหายขึ้นกับระบบสารสนเทศ ข้อมูล เครือข่ายสารสนเทศของทางราชการ เวร ยาม ผู้ดูแลระบบ จะต้องรายงานเหตุให้ผู้บังคับบัญชาทราบ เพื่อให้ผู้บังคับบัญชาสามารถรู้ถึงขอบเขตความเสียหาย และสามารถสั่งการระงับสถานการณ์ฉุกเฉินและความเสียหายได้อย่างรวดเร็วและมีประสิทธิภาพ โดยการรายงานเหตุนี้เบื้องต้น ควรมีอย่างน้อย ๓ วงรอบคือ การรายงานเหตุเบื้องต้น หลังจากที่เกิดเหตุการณ์และได้ทำการวิเคราะห์หาสาเหตุเบื้องต้นแล้ว หลังจากนั้นเมื่อได้ทำการวิเคราะห์หนทางการระงับเหตุหรือความเสียหายแล้ว ควรรายงานให้ผู้บังคับบัญชาทราบถึงแนวทางการดำเนินการในการแก้ไขปัญหา และสุดท้ายเมื่อได้ดำเนินการระงับเหตุและความเสียหายแล้ว จะต้องมีการรายงานการปฏิบัติทั้งหมดในการดำเนินการแก้ไขปัญหาโดยละเอียด เพื่อให้ผู้บังคับบัญชาทราบ และสามารถใช้เป็นแนวทางในการป้องกันเหตุหรือความเสียหายในลักษณะเดียวกับที่จะเกิดขึ้นในอนาคตได้

๔. <u>ขั้นตอนการปฏิบัติ</u> เป็นขั้นตอนการปฏิบัติหรือกระบวนการปฏิบัติจริงรองรับแต่ละสถานการณ์ฉุกเฉิน ขั้นตอนการปฏิบัตินี้ ไม่ควรยึดติดกับตราอักษรของอุปกรณ์ เพราะหากในอนาคตมีการเปลี่ยนทดแทน เป็นอุปกรณ์ตราอักษรอื่น ทำให้ขั้นตอนการปฏิบัติในแผนใช้ไม่ได้ และต้องมีการแก้ไข ซึ่งอาจจะทำได้ยากและใช้เวลาในการปรับปรุงแผนฯ นาน

สรุป

สสท.ทร. ได้จัดทำคู่มือนี้ฉบับนี้ขึ้นเพื่อให้ นขต.ทร. ที่มีระบบสารสนเทศใช้งานภายในหน่วย สามารถใช้เป็นแนวทางในการจัดทำแผนรองรับในกรณีที่เกิดเหตุการณ์ฉุกเฉินขึ้นและส่งผลกระทบต่อการให้บริการของระบบสารสนเทศดังกล่าว เพื่อลดผลกระทบและความเสียหายอันอาจเกิดขึ้นจากการที่ระบบสารสนเทศไม่สามารถใช้งานได้ โดยการจัดทำแผนฯ อย่างมีประสิทธิภาพ จะต้องมีการศึกษาทำความเข้าใจ องค์กร และความสำคัญของระบบสารสนเทศที่องค์กรใช้ รวมทั้งความเสี่ยงที่อาจจะเกิดขึ้นกับระบบสารสนเทศนั้น ๆ เพื่อใช้ในการกำหนดแนวทางการป้องกัน และลดความเสียหายได้อย่างมีประสิทธิภาพ รวมทั้งควรมีการระบุคณะทำงาน หรือทีมงาน รองรับการปฏิบัติรองรับสถานการณ์ฉุกเฉินที่ชัดเจน เพื่อให้การปฏิบัติเป็นไปอย่างมีเอกภาพและมีประสิทธิภาพ ไม่เกิดความสับสนระหว่างผู้เกี่ยวข้อง สำหรับความเสี่ยง และมาตการรองรับความเสี่ยงต่อระบบสารสนเทศนั้น ก็ควรมีการจัดลำดับความสำคัญ ความจำเป็นเร่งด่วนในการดำเนินการ เพื่อให้การปฏิบัติในสถานการณ์ฉุกเฉินเป็นไปอย่างมีประสิทธิภาพและรวดเร็ว

ผนวก

ตัวอย่าง แผนเตรียมความพร้อมกรณีเกิดเหตุฉุกเฉินด้านสารสนเทศ

ศูนย์ข้อมูลกลาง สำนักปฏิบัติการ

กรมการสื่อสารและเทคโนโลยีสารสนเทศทหารเรือ

แผนเตรียมความพร้อมกรณีเกิดเหตุฉุกเฉินด้านสารสนเทศ
ศูนย์ข้อมูลกลาง สำนักปฏิบัติการ
กรมการสื่อสารและเทคโนโลยีสารสนเทศทหารเรือ

อ้างถึง ระเบียบและนโยบายด้านความมั่นคงปลอดภัยที่เกี่ยวข้อง

ก. พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.๒๕๕๐
ข. ระเบียบว่าด้วยการรักษาความลับทางราชการ พ.ศ.๒๕๔๔
ค. ระเบียบสำนักนายกรัฐมนตรีว่าด้วยการรักษาความปลอดภัยแห่งชาติ พ.ศ.๒๕๕๒
ง. ระเบียบกองทัพเรือว่าด้วยการรักษาความปลอดภัย พ.ศ.๒๕๓๑
จ. ระเบียบกองทัพเรือว่าด้วยการรักษาความปลอดภัยระบบสารสนเทศ พ.ศ.๒๕๕๔
ฉ. นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของกองทัพเรือ พ.ศ.๒๕๕๘
ช. แนวทางการใช้งานระบบสารสนเทศของกองทัพเรือ พ.ศ.๒๕๕๘
ซ. อฉก ๑๗๐๐

๑. หลักการและเหตุผล

ปัจจุบัน ทร.ได้นำเอาระบบสารสนเทศเข้ามาใช้เพื่อช่วยเพิ่มประสิทธิภาพในการปฏิบัติราชการ ทั้งระบบสารสนเทศเพื่อการบริหารจัดการ (Management Information System: MIS) และระบบงานสารสนเทศสำหรับงานด้านยุทธการ ซึ่งระบบสารสนเทศหลักของ ทร. หลายระบบ อาทิเช่น ระบบสารบรรณอิเล็กทรอนิกส์ ระบบงานกำลังพล ระบบการบริหารจัดการทรัพยากรองค์กรล้วนแล้วแต่ติดตั้งและให้บริการจากศูนย์ข้อมูลกลางกองทัพเรือ (ศขก.สปก.สสท.ทร.)

เพื่อเป็นการลดโอกาสความเสียหายที่เกิดขึ้นจากเหตุการณ์ไม่พึงประสงค์ รวมทั้งจากสถานการณ์ฉุกเฉินต่าง ๆ การจัดทำแผนเตรียมความพร้อมกรณีเกิดเหตุฉุกเฉินด้านสารสนเทศ จึงเป็นการเตรียมการรับมือกับเหตุการณ์ฉุกเฉินในรูปแบบต่าง ๆ เพื่อให้หน่วยสามารถดำเนินภารกิจได้ในสภาวะวิกฤตได้อย่างมีประสิทธิภาพ สสท.ทร.โดย คณะกรรมการจัดการกรณีเกิดเหตุฉุกเฉินด้านสารสนเทศของศูนย์ข้อมูลกลาง จึงได้จัดทำแผนเตรียมความพร้อมกรณีเกิดเหตุฉุกเฉินด้านสารสนเทศ ของ ศขก.สปก.สสท.ทร. (ศขก.สปก.ฯ) ขึ้น เพื่อเป็นแนวทางในการเตรียมความพร้อมต่อสภาวะวิกฤต และทำให้สามารถใช้งานระบบสารสนเทศหลักของ ทร. และเครือข่ายภายใน ศขก.สปก.ฯ ได้อย่างต่อเนื่องเป็นระบบและมีประสิทธิภาพ

๒. วัตถุประสงค์ (Objectives)

๒.๑ เพื่อใช้เป็นแนวทางในการเตรียมความพร้อมกรณีเกิดเหตุฉุกเฉินด้านสารสนเทศภายใน ศขก.สปก.ฯ
๒.๒ เพื่อลดผลกระทบจากการหยุดชะงักในการดำเนินงานหรือการให้บริการ
๒.๓ เพื่อบรรเทาความเสียหายให้อยู่ระดับที่ยอมรับได้
๒.๔ เพื่อให้ นขต.ทร. และข้าราชการ ทร. มีความเชื่อมั่นในศักยภาพของ ศขก.สปก.ฯ แม้ต้องเผชิญกับเหตุการณ์ร้ายแรงและส่งผลกระทบจนทำให้การดำเนินงานต้องหยุดชะงัก

๓. ขอบเขตการดำเนินการ

แผนนี้พิจารณาจัดการความเสี่ยงด้านเทคนิคและความเสี่ยงทางกายภาพที่เกิดจากภัยหรือสถานการณ์ฉุกเฉินต่อระบบเทคโนโลยีสารสนเทศ ระบบเครือข่ายและข้อมูลภายใน ศขก.สปก.ฯ โดยในแผนนี้ได้พิจารณาแล้วว่าความเสี่ยงต่อผู้ปฏิบัติงาน และความเสี่ยงด้านการบริหารจัดการ ไม่มี เนื่องจาก การจัดทำแผนนี้ ได้รับความเห็นชอบและสนับสนุนทรัพยากรต่าง ๆ จากผู้บังคับบัญชา

๔. ทีมงานบริหารแผนเตรียมความพร้อมกรณีเกิดเหตุฉุกเฉินด้านสารสนเทศของ ศขก.สปก.ฯ

เพื่อให้แผนเตรียมพร้อมกรณีเกิดเหตุฉุกเฉินด้านสารสนเทศ (CP) ของ ศขก.สปก.ฯ สามารถนำไปปฏิบัติได้อย่างมีประสิทธิภาพและเกิดประสิทธิผล จะต้องจัดตั้งทีมงานบริหารความเสี่ยง (CP TEAM) ขึ้น โดย CP TEAM ประกอบด้วยโครงสร้าง และหน้าที่ดังนี้

๑. ผู้บริหารเทคโนโลยีสารสนเทศระดับสูงของ ศขก.สปก.ฯ (DC CIO) มีหน้าที่บริหารงานภายใน ศขก.สปก.ฯ ให้สามารถให้บริการอินเทอร์เน็ต การให้บริการระบบสารสนเทศหลักของ ทร. การรับฝากระบบสารสนเทศของ นขต.ทร. ได้อย่างมีประสิทธิภาพและมั่นคงปลอดภัย

๒. หัวหน้าเจ้าหน้าที่/เจ้าหน้าที่รักษาความปลอดภัยระบบสารสนเทศของ ศขก. สปก.ฯ มีหน้าที่ดำเนินการรักษาความมั่นคงปลอดภัย วิเคราะห์และประเมินความเสี่ยงของระบบที่ให้บริการภายใน ศขก.สปก.ฯ

๓. หัวหน้าเจ้าหน้าที่/เจ้าหน้าที่ควบคุมระบบสารสนเทศของ ศขก.สปก.ฯ มีหน้าที่ให้บริการติดตั้งระบบเครื่องคอมพิวเตอร์แม่ข่าย ตรวจสอบ ควบคุมการทำงาน สำรองและกู้คืนข้อมูลระบบสารสนเทศในระดับระบบปฏิบัติการ

๔. หัวหน้าเจ้าหน้าที่/เจ้าหน้าที่ด้านซอฟท์แวร์ระบบสารสนเทศที่ให้บริการใน ศขก.สปก.ฯ มีหน้าที่บำรุงรักษา วิเคราะห์ ปรับปรุง แก้ไขปัญหาระบบสารสนเทศที่ติดตั้งภายใน ศขก.สปก.ฯ

๕. หัวหน้าเจ้าหน้าที่/เจ้าหน้าที่ตรวจสอบและวิเคราะห์ความเสียหายที่เกิดขึ้นภายใน ศขก.สปก.ฯ มีหน้าที่กำหนดแนวทางและมาตรการรักษาความมั่นคงปลอดภัย ตรวจสอบและวิเคราะห์สาเหตุของความเสียหายที่เกิดขึ้นจากการโจมตีทางไซเบอร์ พร้อมทั้งให้คำแนะนำในแก้ไขปัญหาของระบบที่เกิดจากการโจมตีทางไซเบอร์

๖. หัวหน้าเจ้าหน้าที่/เจ้าหน้าที่ประสานงานกับผู้ดูแลระบบสารสนเทศ นขต.ทร. มีหน้าที่ บริหารระบบผู้ใช้งานระบบสารสนเทศ ทร. ประสานงานการให้บริการ เผยแพร่และควบคุมการให้บริการต่าง ๆ ของ ศขก.สปก.ฯ

โดยทุกตำแหน่งจะต้องร่วมมือกันดูแล ติดตาม ปฏิบัติงาน และกู้คืนเหตุการณ์ฉุกเฉินในส่วนที่รับผิดชอบให้สามารถบริหารแผนฯ และกลับสู่สภาวะปกติได้โดยเร็ว ตามบทบาทหน้าที่ที่กำหนดไว้ของทีมบริหารความเสี่ยง (CP TEAM) และในกรณีที่บุคลากรไม่สามารถปฏิบัติหน้าที่ได้ ให้บุคลากรสำรองรับผิดชอบทำหน้าที่ในหน้าที่ของบุคลากรหลัก ปรากฏดังในตาราง

บุคลากรหลัก		บทบาท	บุคลากรสำรอง	
ชื่อ	**เบอร์โทรศัพท์**		**ชื่อ**	**เบอร์โทรศัพท์**
ผอ.ศขก.สปก.สสท.ทร.	๕๗๘๐๑	ผู้บริหารเทคโนโลยีสารสนเทศระดับสูงของ ศขก.สปก.ฯ	รอง ผอ.ศขก.สปก.ฯ	๕๗๘๐๒
หน.รักษาความปลอดภัย ศขก.สปก.ฯ	๕๗๘๑๖	หัวหน้า จนท. รักษาความปลอดภัยระบบสารสนเทศ ศขก.สปก.ฯ	น.ปฏิบัติการ แผนกรักษาความปลอดภัย ศขก.สปก.ฯ	๕๗๘๑๕
หน.ควบคุม ศขก.สปก.ฯ	๕๗๘๑๒	หัวหน้า จนท. ควบคุมระบบ ศขก.สปก.ฯ	น.ปฏิบัติการแผนกควบคุม ศขก.สปก.ฯ	๕๗๘๑๓
หน.วิเคราะห์ระบบ กพน.สปก.ฯ	๕๗๘๒๓	หัวหน้า จนท. ด้านซอฟท์แวร์ระบบสารสนเทศที่ให้บริการใน ศขก.สปก.ฯ	น.วิเคราะห์ระบบแผนกวิเคราะห์ระบบ กพน.สปก.ฯ	๕๗๘๒๒
หน.รักษาความมั่นคงปลอดภัย กสซ.สปก.ฯ	๕๗๘๘๙	หัวหน้า จนท. ตรวจสอบและวิเคราะห์ความเสียหาย	น.รักษาความมั่นคงปลอดภัย แผนกรักษาความมั่นคงปลอดภัย กสซ.สปก.ฯ	๕๗๘๘๕
หน.บริการสารสนเทศ ศขก.สปก.ฯ	๕๗๘๐๙	หัวหน้า จนท. ประสานงานกับผู้ดูแลระบบสารสนเทศ นขต.ทร.	ประจำแผนกบริการสารสนเทศ ศขก.สปก.ฯ	๕๗๘๐๘

๕. การวิเคราะห์ความเสี่ยง

จากการวิเคราะห์ความเสี่ยงด้านสารสนเทศของหน่วยงานสามารถแยกประเภทความเสี่ยงเป็น ๒ ประเภท ดังนี้

๕.๑ ความเสี่ยงด้านเทคนิค

- การโจมตีทางเครือข่าย/บุกรุกทางเครือข่าย
- DC เครือข่ายเสียหาย (อุปกรณ์ในระบบ)
- เครื่องแม่ข่ายชำรุด
- ระบบปฏิบัติการเสียหาย
- โปรแกรมเสียหาย (application/database)
- เครื่องแม่ข่ายใน DC ติดมัลแวร์/ทำงานผิดปกติ
- ระบบถูกเรียกใช้บริการเต็มขีดความสามารถ
- Shared host มีปัญหา
- ฐานข้อมูล ผู้ดูแลระบบ รั่วไหล (บูรณาการ วงรอบ การแจ้งเตือน สอบถามข้อมูล) จากการโจมตี
- การเชื่อมต่อเครือข่ายที่ตั้ง DC ถูกตัดขาด

๕.๒ ความเสี่ยงด้านกายภาพ

- DC ถูกโจมตีทางกายภาพ/การก่อวินาศกรรม DC
- DC ถูกปิดล้อม
- DC ถูกบุกรุกโดยไม่ได้รับอนุญาต
- ไฟไหม้อาคาร DC/ไฟไหม้ห้อง DC
- DC ไฟฟ้า กฟน. ถูกตัดขาด/DC ไฟฟ้า กฟน.ดับชั่วคราว
- DC แผ่นดินไหว/ภัยธรรมชาติ

๖. ลักษณะรายละเอียดของความเสี่ยง

ชื่อความเสี่ยง	รหัส	ประเภทความเสี่ยง	ลักษณะความเสี่ยง	ปัจจัยเสี่ยง/สิ่งคุกคาม	ผลกระทบ/ผู้ได้รับผลกระทบ
1. การโจมตีทางเครือข่าย/บุกรุกทางเครือข่าย	100	ความเสี่ยงด้านเทคนิค	การเชื่อมต่อไปยังเครื่อง Server มีปัญหา/โปรแกรมทำงานไม่ได้หรือทำงานไม่ถูกต้อง/การเข้าถึงระบบโดยไม่ได้รับอนุญาต	ระบบมีจุดอ่อนต่อการโจมตี	ผู้ใช้งานระบบสารสนเทศ ผู้ดูแลระบบ เจ้าของระบบ
2. DC เครือข่ายเสียหาย	101	ความเสี่ยงด้านเทคนิค	การเชื่อมต่อไปยังเครื่อง Server มีปัญหา	สายสัญญาณ อุปกรณ์เครือข่าย เช่น switch router firewall ชำรุด	ผู้ใช้งานเครือข่าย ผู้ดูแลระบบ เจ้าของระบบ
3. เครื่องแม่ข่ายชำรุด	102	ความเสี่ยงด้านเทคนิค	การเชื่อมต่อไปยังเครื่อง Server มีปัญหา	ฮาร์ดแวร์ชำรุด	ผู้ใช้งานเครือข่าย ผู้ดูแลระบบ เจ้าของระบบ
4. ระบบปฏิบัติการเสียหาย	103	ความเสี่ยงด้านเทคนิค	การเชื่อมต่อไปยังเครื่อง Server มีปัญหา	ระบบปฏิบัติการชำรุด	ผู้ใช้งานเครือข่าย ผู้ดูแลระบบ เจ้าของระบบ
5. โปรแกรมเสียหาย (application/database)	104	ความเสี่ยงด้านเทคนิค	ผู้ใช้เรียกใช้โปรแกรมไม่ได้/โปรแกรมทำงานไม่ถูกต้อง	โปรแกรมชำรุด/ทำงานผิดปกติ	ผู้ใช้งานระบบสารสนเทศ ผู้ดูแลระบบ เจ้าของระบบ
6. เครื่องแม่ข่ายใน DC ติดมัลแวร์/ทำงานผิดปกติ	105	ความเสี่ยงด้านเทคนิค	เครื่องแม่ข่ายทำงานหนัก/สร้าง network traffic ปริมาณมาก	ระบบปฏิบัติการ/โปรแกรมทำงานผิดปกติ	ผู้ใช้งานระบบสารสนเทศ ผู้ดูแลระบบ เจ้าของระบบ
7. ระบบถูกเรียกใช้บริการเต็มขีดความสามารถ	106	ความเสี่ยงด้านเทคนิค	ผู้ใช้งานระบบเข้าใช้บริการไม่ได้	การเข้าใช้งานเกินขีดความสามารถของระบบ (SSO/webserver/DBMS)	ผู้ใช้งานระบบสารสนเทศ ผู้ดูแลระบบ เจ้าของระบบ
8. Shared host มีปัญหา	107	ความเสี่ยงด้านเทคนิค	ระบบ/โปรแกรมใช้งานไม่ได้เนื่องจาก host มีปัญหา	เมื่อมีปัญหาที่เกิดขึ้นในระบบใดระบบหนึ่งบน host จะส่งผลกระทบกับระบบอื่นบน host เดียวกัน	ผู้ใช้งานระบบสารสนเทศ ผู้ดูแลระบบ เจ้าของระบบ
9. ฐานข้อมูลผู้ดูแลระบบรั่วไหล	108	ความเสี่ยงด้านเทคนิค	การเข้าถึงระบบฐานข้อมูลโดยผู้ไม่ได้รับอนุญาต	ข้อมูลถูกนำไปใช้/แก้ไขเปลี่ยนแปลงโดยไม่ได้รับอนุญาต/ไม่มีสิทธิ์	ผู้ใช้งานระบบสารสนเทศ ผู้ดูแลระบบ เจ้าของระบบ

ชื่อความเสี่ยง	รหัส	ประเภทความเสี่ยง	ลักษณะความเสี่ยง	ปัจจัยเสี่ยง/สิ่งคุกคาม	ผลกระทบ/ผู้ได้รับผลกระทบ
10. การเชื่อมต่อเครือข่ายที่ตั้ง DC ถูกตัดขาด (อินเทอร์เน็ต)	109	ความเสี่ยงด้านเทคนิค	ผู้ใช้งานเครือข่ายไม่สามารถเข้าถึงเครือข่ายอินเทอร์เน็ต	ช่องทางการเชื่อมต่อเครือข่ายอินเทอร์เน็ตชำรุด	ผู้ใช้งานเครือข่าย ผู้ดูแลระบบ
11. DC ถูกโจมตีทางกายภาพ/การก่อวินาศกรรม	201	ความเสี่ยงทางกายภาพ	ระบบต่างๆ ใน ศขก.สปก.ฯ ไม่สามารถใช้งานได้	อุปกรณ์ต่างๆ ในห้องศูนย์ข้อมูลกลางชำรุดไม่สามารถใช้งานได้	ผู้ใช้งานระบบสารสนเทศ ผู้ดูแลระบบ เจ้าของระบบ
12. DC ถูกบุกรุกทางกายภาพจากผู้ไม่มีสิทธิ์	202	ความเสี่ยงทางกายภาพ	ระบบต่างๆ ใน ศขก.สปก.ฯ ไม่สามารถใช้งานได้	อุปกรณ์ต่างๆ ในห้องศูนย์ข้อมูลกลางชำรุดไม่สามารถใช้งานได้	ผู้ใช้งานระบบสารสนเทศ ผู้ดูแลระบบ เจ้าของระบบ
13. ที่ตั้ง DC ถูกปิดล้อม	203	ความเสี่ยงทางกายภาพ	ระบบต่างๆ ใน ศขก.สปก.ฯ ไม่สามารถใช้งานได้ (ไม่สามารถส่งกำลังบำรุงได้)	อุปกรณ์ต่างๆ ในห้องศูนย์ข้อมูลกลางไม่สามารถใช้งานได้ เนื่องจากไม่สามารถส่งกำลังบำรุง	ผู้ใช้งานระบบสารสนเทศ ผู้ดูแลระบบ เจ้าของระบบ
14. ไฟไหม้อาคาร DC/ไฟไหม้ห้อง DC	204	ความเสี่ยงทางกายภาพ	ระบบต่างๆ ใน ศขก.สปก.ฯ ไม่สามารถใช้งานได้	อุปกรณ์ต่างๆ ในห้องศูนย์ข้อมูลกลางชำรุดไม่สามารถใช้งานได้	ผู้ใช้งานระบบสารสนเทศ ผู้ดูแลระบบ เจ้าของระบบ
15. DC ไฟฟ้า กฟน. ถูกตัด/DC ไฟฟ้า กฟน. ดับชั่วคราว	205	ความเสี่ยงทางกายภาพ	ระบบต่างๆ ใน ศขก.สปก.ฯ ไม่สามารถใช้งานได้ (ไม่สามารถส่งกำลังบำรุงได้)	อุปกรณ์ต่างๆ ในห้องศูนย์ข้อมูลกลางไม่สามารถใช้งานได้ เนื่องจากไม่สามารถส่งกำลังบำรุง	ผู้ใช้งานระบบสารสนเทศ ผู้ดูแลระบบ เจ้าของระบบ
16. DC แผ่นดินไหว/ภัยธรรมชาติ	206	ความเสี่ยงทางกายภาพ	ระบบต่างๆ ใน ศขก.สปก.ฯ ไม่สามารถใช้งานได้	อุปกรณ์ต่างๆ ในห้องศูนย์ข้อมูลกลางไม่สามารถใช้งานได้	ผู้ใช้งานระบบสารสนเทศ ผู้ดูแลระบบ เจ้าของระบบ

๗. การประมาณความเสี่ยง (การจัดลำดับความเสี่ยง)

ชื่อความเสี่ยง	รหัส	ประเภทความเสี่ยง	ลักษณะความเสี่ยง	ความถี่	ความรุนแรง	ระดับคะแนน
1. การโจมตีทางเครือข่าย/บุกรุกทางเครือข่าย	100	ความเสี่ยงด้านเทคนิค	การเชื่อมต่อไปยัง Server มีปัญหา / โปรแกรมทำงานไม่ได้ หรือทำงานไม่ถูกต้อง/ การเข้าถึงระบบโดยไม่ได้รับอนุญาต	3	5	15
2. DC เครือข่ายเสียหาย	101	ความเสี่ยงด้านเทคนิค	การเชื่อมต่อไปยังเครื่อง Server มีปัญหา	2	5	10
3. เครื่องแม่ข่ายชำรุด	102	ความเสี่ยงด้านเทคนิค	การเชื่อมต่อไปยังเครื่อง Server มีปัญหา	2	5	10
4. ระบบปฏิบัติการเสียหาย	103	ความเสี่ยงด้านเทคนิค	การเชื่อมต่อไปยังเครื่อง Server มีปัญหา	3	5	15
5. โปรแกรมเสียหาย (application/database)	104	ความเสี่ยงด้านเทคนิค	ผู้ใช้เรียกใช้โปรแกรมไม่ได้/ โปรแกรมทำงานไม่ถูกต้อง	2	5	10
6. เครื่องแม่ข่ายใน DC ติดมัลแวร์/ทำงานผิดปกติ	105	ความเสี่ยงด้านเทคนิค	เครื่องแม่ข่ายทำงานหนัก/ สร้าง network traffic ปริมาณมาก	3	5	15
7. ระบบถูกเรียกใช้บริการเต็มขีดความสามารถ	106	ความเสี่ยงด้านเทคนิค	ผู้ใช้งานระบบเข้าใช้บริการไม่ได้	2	5	10
8. Shared host มีปัญหา	107	ความเสี่ยงด้านเทคนิค	ระบบ/โปรแกรมใช้งานไม่ได้เนื่องจาก host มีปัญหา	2	3	6
9. ฐานข้อมูลผู้ดูแลระบบรั่วไหล	108	ความเสี่ยงด้านเทคนิค	การเข้าถึงระบบฐานข้อมูลโดยผู้ไม่ได้รับอนุญาต	3	5	15
10. การเชื่อมต่อเครือข่ายที่ตั้ง DC ถูกตัดขาด	109	ความเสี่ยงด้านเทคนิค	ผู้ใช้งานเครือข่ายไม่สามารถเข้าถึงเครือข่ายอินเทอร์เน็ต	5	1	5
11. DC ถูกโจมตีทางกายภาพ/การก่อวินาศกรรม	201	ความเสี่ยงทางกายภาพ	ระบบต่างๆ ใน ศขก.สปก.ฯ ไม่สามารถใช้งานได้	1	5	5
12. DC ถูกบุกรุกทางกายภาพจากผู้ไม่มีสิทธิ์	202	ความเสี่ยงทางกายภาพ	ระบบต่างๆ ใน ศขก.สปก.ฯ ไม่สามารถใช้งานได้	2	5	10
13. ที่ตั้ง DC ถูกปิดล้อม	203	ความเสี่ยงทางกายภาพ	ระบบต่างๆ ใน ศขก.สปก.ฯ ไม่สามารถใช้งานได้ (ไม่สามารถส่งกำลังบำรุงได้)	1	3	3
14. ไฟไหม้อาคาร DC/ ไฟไหม้ห้อง DC	204	ความเสี่ยงทางกายภาพ	ระบบต่างๆ ใน ศขก.สปก.ฯ ไม่สามารถใช้งานได้	1	5	5
15. DC ไฟฟ้า กฟน.ถูกตัดขาด/ DC ไฟฟ้า กฟน. ดับชั่วคราว	205	ความเสี่ยงทางกายภาพ	ระบบต่างๆ ใน ศขก.สปก.ฯ ไม่สามารถใช้งานได้ (ไม่สามารถส่งกำลังบำรุงได้)	5	1	5
16. DC แผ่นดินไหว/ ภัยธรรมชาติ	206	ความเสี่ยงทางกายภาพ	ระบบต่างๆ ใน ศขก.สปก.ฯ ไม่สามารถใช้งานได้	1	5	5

๘. การจัดการความเสี่ยง

ลำดับ	ความเสี่ยง	ค่าระดับความเสี่ยง	กลยุทธ์การจัดการความเสี่ยง	แนวทางการดำเนินการจัดการความเสี่ยง	ผู้รับผิดชอบ	ระยะเวลาปฏิบัติการ
1.	การโจมตีทางเครือข่าย/บุกรุกทางเครือข่าย	15	ควบคุมความเสี่ยงโดยมีแผนควบคุมความเสี่ยง	- ป้องกัน/ลดจุดอ่อน - เฝ้าระวังการโจมตี - ระงับการโจมตี/จำกัดความเสียหาย - ระบบสำรองขึ้นทดแทน - กู้คืนระบบ/ข้อมูล - วิเคราะห์หาสาเหตุ	กสช.สปก.ฯ ศขก.สปก.ฯ กพน.สปก.ฯ	- ระยะสั้น ๔ ชั่วโมง - ตรวจสอบวิเคราะห์ ๓ วันทำการ
2.	ระบบปฏิบัติการเสียหาย	15	ควบคุมความเสี่ยงโดยมีแผนควบคุมความเสี่ยง	- ป้องกัน/ลดจุดอ่อน - ระบบสำรองขึ้นทดแทน - กู้คืนระบบ/ข้อมูล - วิเคราะห์หาสาเหตุ	ศขก.สปก.ฯ กพน.สปก.ฯ	- ๓ ชั่วโมง กู้คืนระบบปฏิบัติการ - ตรวจสอบวิเคราะห์ ๓ วันทำการ
3.	เครื่องแม่ข่ายใน DC ติดมัลแวร์/ทำงานผิดปกติ	15	ควบคุมความเสี่ยง/ถ่ายโอนความเสี่ยง (ในกรณีที่ระบบมี MA)	- ตรวจสอบ วิเคราะห์หาสาเหตุ - แก้ไข/แจ้งบริษัทคู่สัญญา (MA) - กู้คืนระบบ/ข้อมูล	ศขก.สปก.ฯ บริษัทคู่สัญญา กพน.สปก.ฯ กสช.สปก.ฯ	- ภายใน ๒๔ ชั่วโมง
4.	ฐานข้อมูลผู้ดูแลระบบรั่วไหล	15	ควบคุมความเสี่ยง	- ป้องกัน/ลดจุดอ่อน - เฝ้าระวังการโจมตี - ระงับการโจมตี/จำกัดความเสียหาย - วิเคราะห์หาสาเหตุประเมินความเสียหาย - ระบบสำรองขึ้นทดแทน/กู้คืนระบบ/ข้อมูล	กพน.สปก.ฯ บริษัทคู่สัญญา (MA) ศขก.สปก.ฯ กสช.สปก.ฯ	- ๓ วันทำการ
5.	DC เครือข่ายเสียหาย	10	ควบคุมความเสี่ยง/ถ่ายโอนความเสี่ยง (ในกรณีที่ระบบมี MA)	- ตรวจสอบ วิเคราะห์หาสาเหตุ - แก้ไข/แจ้งบริษัทคู่สัญญา (MA) - กู้คืนระบบ/ข้อมูล	ศขก.สปก.ฯ บริษัทคู่สัญญา (MA)	- ภายใน ๔ ชั่วโมง
6.	เครื่องแม่ข่ายชำรุด	10	ควบคุมความเสี่ยง/ถ่ายโอนความเสี่ยง (ในกรณีที่ระบบมี MA)	- ตรวจสอบ วิเคราะห์หาสาเหตุ - แก้ไข/แจ้งบริษัทคู่สัญญา (MA) - กู้คืนระบบ/ข้อมูล	ศขก.สปก.ฯ บริษัทคู่สัญญา (MA)	- ภายใน ๒๔ ชั่วโมง

ลำดับ	ความเสี่ยง	ค่าระดับความเสี่ยง	กลยุทธ์การจัดการความเสี่ยง	แนวทางการดำเนินการจัดการความเสี่ยง	ผู้รับผิดชอบ	ระยะเวลาปฏิบัติการ
7.	โปรแกรมเสียหาย (application/ database)	10	ควบคุมความเสี่ยง โดยมีแผนควบคุมความเสี่ยง/ ถ่ายโอนความเสี่ยง (MA)	- ป้องกัน/ลดจุดอ่อน - ระบบสำรองขึ้นทดแทน - กู้คืนระบบ/ข้อมูล - วิเคราะห์หาสาเหตุ	กพน.สปก.ฯ ศขก.สปก.ฯ กสช.สปก.ฯ	- ระยะสั้น ๓ ชั่วโมง - ตรวจสอบวิเคราะห์ ๓ วันทำการ (MA)
8.	ระบบถูกเรียกใช้บริการเต็มขีดความสามารถ * สำหรับระบบใหม่ (oracle)	10	ควบคุมความเสี่ยง โดยมีแผนควบคุมความเสี่ยง/ ถ่ายโอนความเสี่ยง/ ยอมรับความเสี่ยง	- วิเคราะห์หาสาเหตุ/ ประเมินจำนวนผู้เข้าใช้งาน - แก้ไขปัญหาเบื้องต้น - ประสานผู้เกี่ยวข้องขอเพิ่มทรัพยากรชั่วคราวในห้วงเวลาที่มีการใช้บริการจำนวนมาก	กพน.สปก.ฯ บริษัทคู่สัญญา (MA) ศขก.สปก.ฯ	- ๒๔ ชั่วโมง
9.	DC ถูกบุกรุกทางกายภาพจากผู้ไม่มีสิทธิ์ (*สำหรับกรณีที่มี ศขก. สำรอง)	10	ควบคุมความเสี่ยง/ ถ่ายโอนความเสี่ยง (ในกรณีที่ระบบมี MA)	- ตรวจสอบ วิเคราะห์หาสาเหตุ - แก้ไข/แจ้งบริษัทคู่สัญญา (MA) - กู้คืนระบบ/ข้อมูล	ศขก.สปก.ฯ บริษัทคู่สัญญา (MA) กพน.สปก.ฯ	- ๑/๒ ชั่วโมง ถ่ายโอนการทำงานไป ศขก. สำรอง
10.	Shared host มีปัญหา	6	ควบคุมความเสี่ยง	- ตรวจสอบ วิเคราะห์หาสาเหตุ - แก้ไขปัญหา - กู้คืนระบบ/ข้อมูล	ศขก.สปก.ฯ กพน.สปก.ฯ	- ๒๔ ชั่วโมง
11.	การเชื่อมต่อเครือข่ายที่ตั้ง DC ถูกตัดขาด	5	ถ่ายโอนความเสี่ยง	- ตรวจสอบ วิเคราะห์หาสาเหตุ - แก้ไข/แจ้งบริษัทคู่สัญญา (MA)	ศขก.สปก.ฯ บริษัทคู่สัญญา (MA)	- ภายใน ๔ ชั่วโมง
12.	DC ถูกโจมตีทางกายภาพ/ การก่อวินาศกรรม	5	ควบคุมความเสี่ยง/ ถ่ายโอนความเสี่ยง (ในกรณีที่ระบบมี MA)	- ตรวจสอบ วิเคราะห์หาสาเหตุ - แก้ไข/แจ้งบริษัทคู่สัญญา (MA) - กู้คืนระบบ/ข้อมูล	ศขก.สปก.ฯ บริษัทคู่สัญญา (MA) กพน.สปก.ฯ	- ๑/๒ ชั่วโมง ถ่ายโอนการทำงานไป ศขก.สำรอง
13.	ไฟไหม้อาคาร DC /ไฟไหม้ห้อง DC	5	ควบคุมความเสี่ยง โดยมีแผนควบคุมความเสี่ยง/ ถ่ายโอนความเสี่ยง (ในกรณีที่ระบบมี MA)	- ตรวจสอบ วิเคราะห์หาสาเหตุ - แก้ไข/แจ้งบริษัทคู่สัญญา (MA) - กู้คืนระบบ/ข้อมูล	ศขก.สปก.ฯ บริษัทคู่สัญญา (MA) กพน.สปก.ฯ	- ๑/๒ ชั่วโมง ถ่ายโอนการทำงานไป ศขก. สำรอง

ลำดับ	ความเสี่ยง	ค่าระดับความเสี่ยง	กลยุทธ์การจัดการความเสี่ยง	แนวทางการดำเนินการจัดการความเสี่ยง	ผู้รับผิดชอบ	ระยะเวลาปฏิบัติการ
14.	DC ไฟฟ้า กฟน. ถูกตัดขาด/ดับชั่วคราว	5	ควบคุมความเสี่ยงโดยมีแผนควบคุมความเสี่ยง	- ลดจุดอ่อน - ระบบสำรองขึ้นทดแทน	ศขก.สปก.ฯ	- ระบบสำรองไฟฟ้า ทำงานได้ต่อเนื่องอย่างน้อย ๔๘ ชั่วโมง
15.	DC แผ่นดินไหว/ภัยธรรมชาติ	5	ควบคุมความเสี่ยงโดยมีแผนควบคุมความเสี่ยง/ถ่ายโอนความเสี่ยง (ในกรณีที่ระบบมี MA)	- ตรวจสอบ วิเคราะห์หาสาเหตุ - แก้ไข/แจ้งบริษัทคู่สัญญา (MA) - กู้คืนระบบ/ข้อมูล	ศขก.สปก.ฯ บริษัทคู่สัญญา (MA) กพน.สปก.ฯ	- ๑/๒ ชั่วโมง ถ่ายโอนการทำงานไป ศขก. สำรอง
16.	ที่ตั้ง DC ถูกปิดล้อม	3	ควบคุมความเสี่ยงโดยมีแผนควบคุมความเสี่ยง	- ลดจุดอ่อน - ระบบสำรองขึ้นทดแทน	ศขก.สปก.ฯ	- ระบบสำรองไฟฟ้าทำงานได้ต่อเนื่องอย่างน้อย ๔๘ ชั่วโมง

๙. แนวทางการปฏิบัติรองรับสถานการณ์ฉุกเฉินด้านสารสนเทศ

๙.๑ การโจมตีทางเครือข่าย/บุกรุกทางเครือข่ายรายละเอียดตาม ผนวก ก
๙.๒ ระบบปฏิบัติการเสียหาย รายละเอียดตาม ผนวก ข
๙.๓ เครื่องแม่ข่ายใน DC ติดมัลแวร์/ทำงานผิดปกติ รายละเอียดตาม ผนวก ค
๙.๔ ฐานข้อมูล ผู้ดูแลระบบ รั่วไหล รายละเอียดตาม ผนวก ง
๙.๕ DC เครือข่ายเสียหาย รายละเอียดตาม ผนวก จ
๙.๖ เครื่องแม่ข่ายชำรุด รายละเอียดตาม ผนวก ฉ
๙.๗ โปรแกรมเสียหาย (application/database) รายละเอียดตาม ผนวก ช
๙.๘ ระบบถูกเรียกใช้บริการเต็มขีดความสามารถ (สำหรับระบบใหม่–oracle) รายละเอียดตาม ผนวก ซ
๙.๙ DC ถูกบุกรุกทางกายภาพจากผู้ไม่มีสิทธิ์ (*สำหรับกรณีที่มี ศขก. สำรอง) รายละเอียดตาม ผนวก ฌ
๙.๑๐ Shared host มีปัญหา รายละเอียดตาม ผนวก ญ
๙.๑๑ การเชื่อมต่อเครือข่ายที่ตั้ง DC ถูกตัดขาด รายละเอียดตาม ผนวก ฎ
๙.๑๒ DC ถูกโจมตีทางกายภาพ/การก่อวินาศกรรม รายละเอียดตาม ผนวก ฏ
๙.๑๓ ไฟไหม้อาคาร DC/ไฟไหม้ห้อง DC รายละเอียดตาม ผนวก ฐ
๙.๑๔ DC ไฟฟ้า กฟน. ถูกตัดขาด/ดับชั่วคราว รายละเอียดตาม ผนวก ฑ
๙.๑๕ DC แผ่นดินไหว/ภัยธรรมชาติ รายละเอียดตาม ผนวก ฒ
๙.๑๖ ที่ตั้ง DC ถูกปิดล้อมรายละเอียดตาม ผนวก ณ

๑๐. แนวทางการปฏิบัติรองรับสถานการณ์ฉุกเฉินอื่น

สำหรับแนวทางการปฏิบัติรองรับสถานการณ์ฉุกเฉินอื่น ๆ นอกเหนือจากที่กล่าวไว้ในข้อ ๙ ให้ ศขก.สปก.ฯ เป็นหน่วยรับผิดชอบการปฏิบัติ

๑๑. คำอธิบายคำย่อและศัพท์เฉพาะ

CIO	Chief Information Officer	หัวหน้าคณะผู้บริหารด้านสารสนเทศ
CP	Contingency Plan	แผนเตรียมความพร้อมกรณีเกิดเหตุฉุกเฉิน
DC	Data Center	ศูนย์ข้อมูลกลาง
MA	Maintenance Agreement	สัญญาบำรุงรักษาระบบ
MIS	Management Information System	ระบบสารสนเทศเพื่อการบริหารจัดการ
Shared Host		การให้บริการวางเว็บไซต์ร่วม (หนึ่งเครื่องแม่ข่ายให้บริการหลายเว็บไซต์)
SSO	Single Sign On	การยืนยันตัวบุคคลแบบรวมศูนย์

ผนวก ก

มาตรการรองรับการโจมตีทางเครือข่าย/บุกรุกเครือข่าย

๑. ผู้สั่งการในที่เกิดเหตุ: กสซ.สปก.สสท.ทร.

๒. การตรวจสอบและสรุปหาสาเหตุเบื้องต้น

- ได้รับการแจ้งเตือนจากผู้ประสบเหตุ (ทั้งผู้ใช้ทั่วไป/เจ้าของระบบ/ผู้ดูแลระบบ)
- ตรวจสอบ LOG (ศขก.สปก.ฯ: เครือข่าย/รปภ., กพน.สปก.ฯ: ระบบ)
- ตรวจสอบความเสียหายของระบบที่ถูกโจมตี
- ตรวจสอบแหล่งที่มาของการโจมตี

๓. การรายงานเหตุ

- รายงานการตรวจสอบและสรุปหาสาเหตุเบื้องต้นให้ DC-CIO ทราบในโอกาสแรก
- วิเคราะห์หาสาเหตุและเสนอแนะหนทางการแก้ไขปัญหา
- รายงานการปฏิบัติทั้งหมดในการแก้ปัญหา

๔. ขั้นตอนการปฏิบัติ

- ป้องกัน/ลดจุดอ่อน
- เฝ้าระวังการโจมตี
- ระงับการโจมตี/จำกัดความเสียหาย
- ระบบสำรองขึ้นทดแทน
- กู้คืนระบบ/ข้อมูล

ผนวก ข

มาตรการรองรับ DC ระบบปฏิบัติการเสียหาย

๑. ผู้สั่งการในที่เกิดเหตุ: ศขก.สปก.สสท.ทร.

๒. การตรวจสอบและสรุปหาสาเหตุเบื้องต้น

- ตรวจสอบมอนิเตอร์ของศูนย์ข้อมูลกลางว่ามีเครื่องแม่ข่ายเปลี่ยนเป็นสีแดงหรือไม่
    - ไม่มีสีแดง แสดงว่าเครือข่ายใช้งานได้
    - มีสีแดง เจ้าหน้าที่แผนกควบคุม ศขก.สปก.ฯ ตรวจสอบและทำการแก้ไขเครือข่ายภายในศูนย์ข้อมูลกลาง โดยเฉพาะเส้นทางจากเครื่องผู้ใช้งาน (นอกห้องเครื่องแม่ข่าย) ไปยังเครื่องแม่ข่ายนั้น ๆ ตลอดเส้นทางให้สามารถใช้งานได้
- ได้รับการแจ้งเตือนจากผู้ประสบเหตุ (ทั้งผู้ใช้ทั่วไป/เจ้าของระบบ/ผู้ดูแลระบบ)
- ตรวจสอบ LOG (ศขก.สปก.ฯ – เครือข่าย)

๓. การรายงานเหตุ

- รายงานการตรวจสอบและสรุปหาสาเหตุเบื้องต้นให้ DC-CIO ทราบในโอกาสแรก
- วิเคราะห์หาสาเหตุและเสนอแนะหนทางการแก้ไขปัญหา
- รายงานการปฏิบัติทั้งหมดในการแก้ปัญหา

๔. ขั้นตอนการปฏิบัติ

- ตรวจสอบเส้นทางเครือข่าย
- เปลี่ยนอุปกรณ์สำรอง
- แจ้งผู้รับจ้าง MA

ผนวก ค

มาตรการรองรับเครื่องแม่ข่ายใน DC ติดมัลแวร์/ทำงานผิดปกติ

๑ . ผู้สั่งการในที่เกิดเหตุ: ศขก.สปก.สสท.ทร.

๒. การตรวจสอบและสรุปหาสาเหตุเบื้องต้น

- รับแจ้งจากผู้ใช้งาน/ตรวจพบ ตรวจสอบระบบที่ทำงานไม่ปกติ
- แผนก รปภ.ศขก.สปก.ฯ ตรวจสอบการติดตั้ง Anti Malware/Anti Virus และการ Update ต่าง ๆ
- แผนก รปภ.ศขก.สปก.ฯ ตรวจสอบการทำงานของระบบสารสนเทศที่ติดตั้งบนเครื่องแม่ข่าย

๓. การรายงานเหตุ

- รายงานการตรวจสอบและสรุปหาสาเหตุเบื้องต้นให้ DC-CIO ทราบในโอกาสแรก
- วิเคราะห์หาสาเหตุและเสนอแนะหนทางการแก้ไขปัญหา
- รายงานการปฏิบัติทั้งหมดในการแก้ปัญหา

๔. ขั้นตอนการปฏิบัติ

- สำรองข้อมูลเครื่องแม่ข่ายที่มีปัญหา
- ตรวจสอบระบบที่ทำงานไม่ปกติ (OS ระบบงาน เครือข่าย และระบบอื่นๆ ที่เกี่ยวข้อง)/แจ้งเจ้าของระบบงานที่ติดตั้งบนเครื่องแม่ข่าย ดำเนินการตรวจสอบข้อมูลและขั้นตอนการทำงานต่าง ๆ
- แจ้งบริษัทผู้รับจ้าง MA เข้าดำเนินการแก้ไข/ติดตั้ง Anti Virus และ Scan ตรวจสอบมัลแวร์
- ตรวจสอบการทำงานของระบบสารสนเทศที่ติดตั้ง หลังดำเนินการกำจัดมัลแวร์เรียบร้อยแล้ว
- หากระบบยังไม่สามารถใช้งานได้ นำข้อมูลที่สำรองไว้มาใช้งาน
- ติดตามการปรับปรุงซอฟต์แวร์ (OS Anti Virus ฯลฯ) และดำเนินการปรับปรุงซอฟต์แวร์ให้ทันสมัยอยู่เสมอ

ผนวก ง

มาตรการรองรับฐานข้อมูล ผู้ดูแลระบบ รั่วไหล

๑. ผู้สั่งการในที่เกิดเหตุ: กพน.สปก.สสท.ทร.

๒. การตรวจสอบและสรุปหาสาเหตุเบื้องต้น

- ได้รับการแจ้งเตือนจากผู้ประสบเหตุ (ทั้งผู้ใช้ทั่วไป/เจ้าของระบบ/ผู้ดูแลระบบ)
- แผนกบำรุงรักษาระบบ กพน.สปก.ฯ ตรวจสอบ LOG (ศขก.สปก.ฯ – เครือข่าย/รปภ., กพน.สปก.ฯ – ระบบ)
- แผนกบำรุงรักษาระบบ กพน.สปก.ฯ ตรวจสอบความเสียหายที่เกิดขึ้น
- แผนกบำรุงรักษาระบบ กพน.สปก.ฯ ตรวจสอบแหล่งที่มาของผู้ละเมิด

๓. การรายงานเหตุ

- รายงานการตรวจสอบและสรุปหาสาเหตุเบื้องต้นให้ DC-CIO ทราบในโอกาสแรก
- วิเคราะห์หาสาเหตุและเสนอแนะหนทางการแก้ไขปัญหา
- รายงานการปฏิบัติทั้งหมดในการแก้ปัญหา

๔. ขั้นตอนการปฏิบัติ

- แผนกบำรุงรักษาระบบ กพน.สปก.ฯ ประเมินความเสียหาย และประสานหน่วยงานที่เกี่ยวข้อง ศขก.สปก.ฯ กสซ.สปก.ฯ และ บริษัทคู่สัญญา ถ้ามี
- ปิดกั้นจุดอ่อน หรือสาเหตุทำให้เกิดความเสียหาย เลือกคู่มือที่ใช้ประกอบการกู้คืน
    - กรณีที่ ฐานข้อมูลระบบงานเสียหายจากปัจจัยภายนอก เจ้าหน้าที่บำรุงรักษาระบบ แจ้งให้หน่วยเจ้าของระบบทราบให้ดำเนินการเปลี่ยนรหัสผ่านทันที หรือผู้จัดการฐานข้อมูล (DBA) ทำการปิดกั้นช่องทางการเข้าถึงฐานข้อมูล แจ้งให้ กสซ.สปก.ฯ ตรวจจับความเคลื่อนไหวของผู้ไม่ประสงค์ดีที่มาจากภายนอก
    - กรณีที่ ฐานข้อมูลระบบงานเสียหายจากปัจจัยภายในแผนกบำรุงรักษาระบบ กพน.สปก.ฯ จะทำหน้าที่ในการเรียกไฟล์ข้อมูลที่ได้มีการสำรองไว้ เพื่อนำไปใช้ในการกู้คืน
- แผนกบำรุงรักษาระบบ กพน.สปก.ฯ ทำหน้าที่ในการกู้คืนฐานข้อมูล

ผนวก จ

มาตรการรองรับ DC เครือข่ายเสียหาย

๑. ผู้สั่งการในที่เกิดเหตุ: ศขก.สปก.สสท.ทร.

๒. การตรวจสอบและสรุปหาสาเหตุเบื้องต้น

- ตรวจสอบมอนิเตอร์ของศูนย์ข้อมูลกลางว่ามีเครื่องแม่ข่ายเปลี่ยนเป็นสีแดงหรือไม่
    - ไม่มีสีแดง แสดงว่าเครือข่ายใช้งานได้
    - มีสีแดง เจ้าหน้าที่แผนกควบคุม ศขก.สปก.ฯ ตรวจสอบและทำการแก้ไขเครือข่ายภายในศูนย์ข้อมูลกลาง โดยเฉพาะเส้นทางจากเครื่องผู้ใช้งาน (นอกห้องเครื่องแม่ข่าย) ไปยังเครื่องแม่ข่ายนั้น ๆ ตลอดเส้นทางให้สามารถใช้งานได้
- ได้รับการแจ้งเตือนจากผู้ประสบเหตุ (ทั้งผู้ใช้ทั่วไป/เจ้าของระบบ/ผู้ดูแลระบบ)
- ตรวจสอบ LOG (ศขก.สปก.ฯ – เครือข่าย)

๓. การรายงานเหตุ

- รายงานการตรวจสอบและสรุปหาสาเหตุเบื้องต้นให้ DC-CIO ทราบในโอกาสแรก
- วิเคราะห์หาสาเหตุและเสนอแนะหนทางการแก้ไขปัญหา
- รายงานการปฏิบัติทั้งหมดในการแก้ปัญหา

๔. ขั้นตอนการปฏิบัติ

- ตรวจสอบเส้นทางเครือข่าย
- เปลี่ยนอุปกรณ์สำรอง
- แจ้งผู้รับจ้าง MA

ผนวก ฉ
มาตรการรองรับเครื่องแม่ข่ายชำรุด

๑. ผู้สั่งการในที่เกิดเหตุ: ศขก.สปก.สสท.ทร.

๒. การตรวจสอบและสรุปหาสาเหตุเบื้องต้น

- รับแจ้ง ระบบใช้งานไม่ได้ ดูมอนิเตอร์ของ ศขก.สปก.ฯ มีเครื่องแม่ข่ายที่เป็นสีแดง
- แผนกควบคุม ศขก.สปก.ฯ ตรวจสอบเครื่องแม่ข่ายอื่นที่อยู่ในเครือข่ายเดียวกันยังใช้งานได้
- แผนกควบคุม ศขก.สปก.ฯ เข้าตรวจสอบเครื่องแม่ข่ายที่มีปัญหา

๓. การรายงานเหตุ

- รายงานการตรวจสอบและสรุปหาสาเหตุเบื้องต้นให้ DC-CIO ทราบในโอกาสแรก
- วิเคราะห์หาสาเหตุและเสนอแนะหนทางการแก้ไขปัญหา
- รายงานการปฏิบัติทั้งหมดในการแก้ปัญหา

๔. ขั้นตอนการปฏิบัติ

- ตรวจสอบมอนิเตอร์ของแผนกควบคุม ศขก.สปก.ฯ มีเครื่องแม่ข่ายเปลี่ยนเป็นสีแดง และเครื่องแม่ข่ายที่อยู่ในเครือข่ายเดียวกันยังสามารถใช้งานได้
- เข้าทำการตรวจสอบทางกายภาพของเครื่องแม่ข่ายที่มีปัญหา/แจ้งผู้รับจ้าง MA ให้ดำเนินการตรวจสอบและแก้ไข
- ดำเนินการเปลี่ยนเครื่องแม่ข่าย นำข้อมูลและระบบเดิมกลับมาใช้งาน

ผนวก ช

มาตรการรองรับโปรแกรมเสียหาย (application/database)

๑. ผู้สั่งการในที่เกิดเหตุ: กพน.สปก.สสท.ทร.

๒. การตรวจสอบและสรุปหาสาเหตุเบื้องต้น

- ได้รับการแจ้งเตือนจากผู้ประสบเหตุ (ทั้งผู้ใช้ทั่วไป/เจ้าของระบบ/ผู้ดูแลระบบ)
- แผนกโปรแกรม กพน.สปก.ฯ ตรวจสอบความเสียหายของระบบ/ตรวจสอบ LOG ของระบบ
- แผนกโปรแกรม กพน.สปก.ฯ ตรวจสอบหาสาเหตุของปัญหา

๓. การรายงานเหตุ

- รายงานการตรวจสอบและสรุปหาสาเหตุเบื้องต้นให้ DC-CIO ทราบในโอกาสแรก
- วิเคราะห์หาสาเหตุและเสนอแนะหนทางการแก้ไขปัญหา
- รายงานการปฏิบัติทั้งหมดในการแก้ปัญหา

๔. ขั้นตอนการปฏิบัติ

- แผนกโปรแกรม กพน.สปก.ฯ ประเมินความเสียหาย และประสานหน่วยงานที่เกี่ยวข้อง ศขก.สปก.ฯ กสซ.สปก.ฯ และ บริษัทคู่สัญญา ถ้ามี
- ปิดกั้นจุดอ่อน หรือสาเหตุทำให้เกิดความเสียหาย
    - กรณีที่ โปรแกรมที่ กพน.สปก.ฯ รับผิดชอบ ดำเนินการแก้ไข/แจ้ง MA
    - กรณีที่ โปรแกรมเป็นของ หน่วยอื่นรับผิดชอบ แผนกโปรแกรม แจ้งหน่วยเจ้าของโปรแกรม
- กู้คืนระบบ

ผนวก ซ

มาตรการรองรับระบบถูกเรียกใช้บริการเต็มขีดความสามารถ

๑. ผู้สั่งการในที่เกิดเหตุ: กพน.สปก.สสท.ทร.

๒. การตรวจสอบและสรุปหาสาเหตุเบื้องต้น

- ได้รับการแจ้งเตือนจากผู้ประสบเหตุ (ทั้งผู้ใช้ทั่วไป/เจ้าของระบบ/ผู้ดูแลระบบ)
- แผนกวิเคราะห์ระบบ กพน.สปก.ฯ ตรวจสอบ LOG โดยประสานขอข้อมูล LOG จาก ศขก.สปก.ฯ
- แผนกวิเคราะห์ระบบ กพน.สปก.ฯ ตรวจสอบหาสาเหตุของปัญหา

๓. การรายงานเหตุ

- รายงานการตรวจสอบและสรุปหาสาเหตุเบื้องต้นให้ DC-CIO ทราบในโอกาสแรก
- วิเคราะห์หาสาเหตุและเสนอแนะหนทางการแก้ไขปัญหา
- รายงานการปฏิบัติทั้งหมดในการแก้ปัญหา

๔. ขั้นตอนการปฏิบัติ

- แผนกวิเคราะห์ระบบม กพน.สปก.ฯ ประเมินหาสาเหตุของการใช้งานเต็มขีดความสามารถของระบบ
- ประสาน ศขก.สปก.ฯ ขอเพิ่มทรัพยากร รองรับการใช้งานที่เพิ่มขึ้นชั่วคราว
- ประสานหน่วยเกี่ยวข้องกำหนดห้วงเวลาการใช้งานให้รองรับการให้บริการของระบบ (การประเมินต่างๆ)

<u>หมายเหตุ</u> ระบบของ กพน.สปก.ฯ สามารถรองรับการใช้งานได้ผู้งานจำนวน ๒๕๖ คนในเวลาเดียวกัน (concurrent user) และจะเพิ่มเป็น ๑,๐๐๐ คนในเวลาเดียวกัน ในปี งป.๕๙

ผนวก ฌ

มาตรการรองรับDC ถูกบุกรุกทางกายภาพจากผู้ไม่มีสิทธิ์

๑. ผู้สั่งการในที่เกิดเหตุ: ศขก.สปก.สสท.ทร.

๒. การตรวจสอบและสรุปหาสาเหตุเบื้องต้น

- มี SMS แจ้งเตือนว่ามีการเปิดปิดประตูที่มี Security Access
- แผนก รปภ.ศขก.สปก.ฯ ตรวจสอบกล้องวงจรปิดใน ศขก.สปก.ฯ
- ตรวจสอบระบบต่าง ๆ ใช้งานไม่ได้

๓. การรายงานเหตุ

- รายงานการตรวจสอบและสรุปหาสาเหตุเบื้องต้นให้ DC-CIO ทราบในโอกาสแรก
- วิเคราะห์หาสาเหตุและเสนอแนะหนทางการแก้ไขปัญหา
- รายงานการปฏิบัติทั้งหมดในการแก้ปัญหา

๔. ขั้นตอนการปฏิบัติ

- มี SMS แจ้งเตือนว่ามีการเปิดปิดประตูภายในห้อง DC
- ตรวจสอบผู้เข้าใช้งานผ่านระบบ Access Control และกล้องวงจรปิด
- สอบสวนผู้ที่เกี่ยวข้อง
- ทบทวนมาตรการรักษาความปลอดภัย แก้ไข และอนุมัติใช้งาน
- กรณีเกิดความเสียหายจนไม่สามารถให้บริการได้ ให้ถ่ายโอนการให้บริการไปยัง ศขก. สำรอง (กรณีที่มี ศขก.สำรอง)

ผนวก ญ

มาตรการรองรับ Shared host มีปัญหา

๑. ผู้สั่งการในที่เกิดเหตุ: ศขก.สปก.สสท.ทร.

๒. การตรวจสอบและสรุปหาสาเหตุเบื้องต้น

- ได้รับการแจ้งเตือนจากผู้ประสบเหตุ (ทั้งผู้ใช้ทั่วไป/เจ้าของระบบ/ผู้ดูแลระบบ) ระบบใช้งานไม่ได้
- แผนกควบคุม ศขก.สปก.ฯ ตรวจสอบระบบมอนิเตอร์
- ตรวจสอบระบบที่ติดตั้งร่วมกับระบบที่มีปัญหา

๓. การรายงานเหตุ

- รายงานการตรวจสอบและสรุปหาสาเหตุเบื้องต้นให้ DC-CIO ทราบในโอกาสแรก
- วิเคราะห์หาสาเหตุและเสนอแนะหนทางการแก้ไขปัญหา
- รายงานการปฏิบัติทั้งหมดในการแก้ปัญหา
- แจ้งเจ้าของระบบทั้งหมดที่ติดตั้งอยู่บนเครื่องแม่ข่ายนั้น

๔. ขั้นตอนการปฏิบัติ

- แผนกควบคุม ศขก.สปก.ฯ ทำการสำรองข้อมูลของ Host ที่มีปัญหา
- แผนกควบคุม ศขก.สปก.ฯ ตรวจสอบ วิเคราะห์ หาสาเหตุ และแก้ไขปัญหา
- แผนกควบคุม ศขก.สปก.ฯ แจ้งผู้ดูแลแต่ละระบบ สาเหตุ และแนวทางการแก้ไขปัญหา
- แผนกควบคุม ศขก.สปก.ฯ สร้าง Host ใหม่ ติดตั้งระบบปฏิบัติการ เซอร์วิสต่าง ๆ พร้อมทั้งกำหนดค่า Config ต่าง ๆ
- แผนกควบคุม ศขก.สปก.ฯ นำข้อมูล และระบบที่สำรองไว้มาติดตั้งใช้งาน

ผนวก ฎ
มาตรการรองรับการเชื่อมต่อเครือข่ายที่ตั้ง DC ถูกตัดขาด (อินเตอร์เน็ต)

๑. ผู้สั่งการในที่เกิดเหตุ: ศขก.สปก.สสท.ทร.

๒. การตรวจสอบและสรุปหาสาเหตุเบื้องต้น

- ได้รับการแจ้งเตือนจากผู้ประสบเหตุ (ทั้งผู้ใช้ทั่วไป/เจ้าของระบบ/ผู้ดูแลระบบ) ว่าไม่สามารถใช้งานอินเตอร์เน็ตได้
- แผนกควบคุม ศขก.สปก.ฯ ตรวจสอบระบบ อินเตอร์เน็ต

๓. การรายงานเหตุ

- รายงานการตรวจสอบและสรุปหาสาเหตุเบื้องต้นให้ DC-CIO ทราบในโอกาสแรก
- วิเคราะห์หาสาเหตุและเสนอแนะหนทางการแก้ไขปัญหา
- รายงานการปฏิบัติทั้งหมดในการแก้ปัญหา

๔. ขั้นตอนการปฏิบัติ

- แผนกควบคุม ศขก.สปก.ฯ แจ้งบริษัทคู่สัญญาผู้ให้บริการ ดำเนินการแก้ไข

ผนวก ฏ

มาตรการรองรับ DC ถูกโจมตีทางกายภาพ/การก่อวินาศกรรม

๑. ผู้สั่งการในที่เกิดเหตุ: ศขก.สปก.สสท.ทร.

๒. การตรวจสอบและสรุปหาสาเหตุเบื้องต้น

- รับแจ้งจากผู้ใช้งาน/ตรวจพบ การถูกโจมตีทางกายภาพ/การก่อวินาศกรรม
- ศขก.สปก.ฯ ตรวจสอบความเสียหายทางกายภาพที่เกิดภายใน ศขก.สปก.ฯ

๓. การรายงานเหตุ

- รายงานการตรวจสอบและสรุปหาสาเหตุเบื้องต้นให้ DC-CIO ทราบในโอกาสแรก
- วิเคราะห์หาสาเหตุและเสนอแนะหนทางการแก้ไขปัญหา
- รายงานการปฏิบัติทั้งหมดในการแก้ปัญหา

๔. ขั้นตอนการปฏิบัติ

- แผนกควบคุมระบบ ศขก.สปก.ฯ ตรวจสอบและประเมินความเสียหาย ที่เกิดภายใน ศขก.สปก.ฯ
    - เข้าตรวจสอบอุปกรณ์ทั้งหมด ถ้าไม่เสียหาย ดำเนินการกู้ระบบทั้งหมดกลับมาใช้งาน
    - ในกรณีที่เกิดความเสียหายจนไม่สามารถให้บริการได้ สำรองข้อมูล ปิดระบบ ทั้งหมด และทำการย้ายการให้บริการไป ศขก. สำรอง (กรณีที่มี ศขก.สำรอง)

ผนวก ฐ
มาตรการรองรับไฟไหม้อาคาร DC/ไฟไหม้ห้อง DC

๑. ผู้สั่งการในที่เกิดเหตุ: ศขก.สปก.สสท.ทร.

๒. การตรวจสอบและสรุปหาสาเหตุเบื้องต้น

- ระบบแจ้งเตือนอัคคีภัยอัตโนมัติทำงาน
- รับแจ้งว่าไฟไหม้อาคาร/ห้อง DC

๓. การรายงานเหตุ

- รายงานการตรวจสอบและสรุปหาสาเหตุเบื้องต้นให้ DC-CIO ทราบในโอกาสแรก
- วิเคราะห์หาสาเหตุและเสนอแนะหนทางการแก้ไขปัญหา
- รายงานการปฏิบัติทั้งหมดในการแก้ปัญหา

๔. ขั้นตอนการปฏิบัติ

- ดำเนินตามมาตรการด้าน รปภ.
- ระบบดับเพลิงภายในห้องเครื่องแม่ข่ายทำงานโดยอัตโนมัติ
- แผนกควบคุมระบบ ศขก.สปก.ฯ ตรวจสอบและประเมินความเสียหาย ที่เกิดภายใน ศขก.สปก.ฯ
    - เข้าตรวจสอบอุปกรณ์ทั้งหมด ถ้าไม่เสียหาย ดำเนินการกู้ระบบทั้งหมดกลับมาใช้งาน
    - ในกรณีที่เกิดความเสียหายจนไม่สามารถให้บริการได้ สำรองข้อมูล ปิดระบบ ทั้งหมด และทำการย้ายการให้บริการไป ศขก. สำรอง (กรณีที่มี ศขก.สำรอง)

ผนวก ฑ

มาตรการรองรับDC ไฟฟ้า กฟน.ถูกตัดขาด/ ดับชั่วคราว

๑. ผู้สั่งการในที่เกิดเหตุ: ศขก.สปก.สสท.ทร.

๒. การตรวจสอบและสรุปหาสาเหตุเบื้องต้น

- ไฟในส่วนสำนักงานดับ
- เครื่องสำรองไฟฟ้าทำงาน

๓. การรายงานเหตุ

- รายงานการตรวจสอบและสรุปหาสาเหตุเบื้องต้นให้ DC-CIO ทราบในโอกาสแรก
- วิเคราะห์หาสาเหตุและเสนอแนะหนทางการแก้ไขปัญหา
- รายงานการปฏิบัติทั้งหมดในการแก้ปัญหา

๔. ขั้นตอนการปฏิบัติ

- เมื่อไฟดับเกิน ๓๐ วินาที เครื่อง Generator จะทำงานและจ่ายไฟให้ DC
- ตรวจสอบแผงไฟฟ้าที่ห้อง Electric Room ว่า Main Breaker อยู่ที่ตำแหน่ง On หรือไม่ ถ้าไม่อยู่ที่ On (ระบบทำความเย็นไม่ทำงาน) ให้ทำการโยกมาที่ Off แล้ว โยกคืนไปที่ On
- ตรวจสอบระบบทำความเย็นว่าทำงานหรือไม่ ถ้าทำงานแสดงว่าระบบไฟฟ้าสำรองทำงานปกติแล้ว
- ตรวจสอบระดับน้ำมันเชื้อเพลิงของเครื่อง Generator หากไฟดับเกิน ๒ ชั่วโมง
- ดำเนินการเรื่องการส่งกำลังบำรุง (น้ำมันเชื้อเพลิงของเครื่อง Generator)

ผนวก ฒ

มาตรการรองรับ DC แผ่นดินไหว/ภัยธรรมชาติ

๑. ผู้สั่งการในที่เกิดเหตุ: ศขก.สปก.สสท.ทร.

๒. การตรวจสอบและสรุปหาสาเหตุเบื้องต้น

- รับแจ้งจากผู้ใช้งาน/ตรวจพบ แผนดินไหว/ภัยธรรมชาติ
- ศขก.สปก.ฯ ตรวจสอบความเสียหายทางกายภาพที่เกิดภายใน ศขก.สปก.ฯ

๓. การรายงานเหตุ

- รายงานการตรวจสอบและสรุปหาสาเหตุเบื้องต้นให้ DC-CIO ทราบในโอกาสแรก
- วิเคราะห์หาสาเหตุและเสนอแนะหนทางการแก้ไขปัญหา
- รายงานการปฏิบัติทั้งหมดในการแก้ปัญหา

๔. ขั้นตอนการปฏิบัติ

- แผนกควบคุมระบบ ศขก.สปก.ฯ ตรวจสอบและประเมินความเสียหาย ที่เกิดภายใน ศขก.สปก.ฯ
    - เข้าตรวจสอบอุปกรณ์ทั้งหมด ถ้าไม่เสียหาย ดำเนินการกู้ระบบทั้งหมดกลับมาใช้งาน
    - ในกรณีที่เกิดความเสียหายจนไม่สามารถให้บริการได้ สำรองข้อมูล ปิดระบบ ทั้งหมด และทำการย้ายการให้บริการไป ศขก. สำรอง (กรณีที่มี ศขก.สำรอง)

ผนวก ณ
มาตรการรองรับที่ตั้ง DC ถูกปิดล้อม

๑. ผู้สั่งการในที่เกิดเหตุ: ศขก.สปก.สสท.ทร.

๒. การตรวจสอบและสรุปหาสาเหตุเบื้องต้น

- รับแจ้งจากผู้ใช้งาน/ตรวจพบ การปิดล้อมที่ตั้ง DC
- ตรวจสอบผลกระทบที่เกิดจากการปิดล้อม (การเชื่อมต่อ อินเตอร์เน็ต ระบบไฟฟ้า ความเสียหายทางกายภาพ)

๓. การรายงานเหตุ

- รายงานการตรวจสอบและสรุปหาสาเหตุเบื้องต้นให้ DC-CIO ทราบในโอกาสแรก
- วิเคราะห์หาสาเหตุและเสนอแนะหนทางการแก้ไขปัญหา
- รายงานการปฏิบัติทั้งหมดในการแก้ปัญหา

๔. ขั้นตอนการปฏิบัติ

- ให้ดูขั้นตอนการปฏิบัติตามผนวกที่เกี่ยวข้อง