แผนกู้คืนระบบสารสนเทศ

Disaster Recovery Plan (DRP)

กลุ่มบริษัท ดิทโต้ (ประเทศไทย) จำกัด (มหาชน)

1 เมษายน 2563

ผู้จัดทำ	ผู้ตรวจสอบ	ผู้อนุมัติ
พิพัฒน์ รุจิวศิน		
(นายพิพัฒน์ รุจิวศิน)	(นายติณณ์ภพ ไพรสณฑ์)	(นายฐกร รัตนกมลพร)
เจ้าหน้าที่เทคโนโลยีสารสนเทศ	ผู้จัดการแผนกเทคโนโลยีสารสนเทศ	ประธานเจ้าหน้าที่บริหาร

1. หลักการและเหตุผล

ปัจจุบันภัยที่เกิดแก่ระบบเทคโนโลยีสารสนเทศมีอัตราการเกิดเพิ่มขึ้น ตามความก้าวหน้าของเทคโนโลยี สารสนเทศ ภัยอันตรายที่เกิดขึ้นกับระบบเทคโนโลยีสารสนเทศอาจเกิดขึ้นได้โดยคน ซึ่งได้แก่ เจ้าหน้าที่ บุคลากร ของหน่วยงานที่เกี่ยวข้องกับการใช้งานเทคโนโลยีสารสนเทศ หรือบุคคลภายนอกองค์กรโดยอาศัย สถานการณ์ หรือเหตุการณ์ ทั้งเจตนาและไม่เจตนา อันเป็นเหตุให้ข้อมูลข่าวสารในระบบเทคโนโลยีสารสนเทศถูกเปิดเผย หรือ เปลี่ยนแปลงทำลาย ปฏิเสธการทำงาน หรือการกระทำอื่นๆ ตามความต้องการของภัย และภัยอันตรายที่เกิดจากภัย ธรรมชาติ อันได้แก่ อัคคีภัย วาตภัย อุทกภัย เป็นต้น ดังนั้น เพื่อเป็นการลดภัยอันตรายดังกล่าว ทั้งสองประเภทที่ จะเกิดขึ้นกับระบบเทคโนโลยีสารสนเทศ จึงเห็นความจำเป็นอย่างยิ่งที่กลุ่มบริษัท ดิทโต้ (ประเทศไทย) จำกัด (มหาชน) จะต้องมี แผนและคู่มือปฏิบัติการเพื่อรองรับสถานการณ์ฉุกเฉินจากภัยพิบัติที่อาจจะเกิดขึ้น จากเหตุผลข้างต้น ทางฝ่ายเทคโนโลยีสารสนเทศ จึงได้ประเมินสถานการณ์จากปัจจัยที่มี โอกาสเกิดกับระบบเทคโนโลยีสารสนเทศ รวมถึงการจัดทำแผนปฏิบัติเพื่อรับสถานการณ์ที่ได้ประเมินโดยแบ่งออกเป็น 3 ด้าน ได้แก่ แผนการรองรับสถานการณ์ฉุกเฉินจากภัยพิบัติที่เกิดขึ้นกับระบบห้องคอมพิวเตอร์แม่ข่ายและระบบเครือข่ายคอมพิวเตอร์ (Contingency Plan) แผนการดำเนินการเพื่อให้ระบบเครือข่ายคอมพิวเตอร์ใช้งานได้อย่างต่อเนื่อง (Continuity of Operation Plan) และแผนการฟื้นตัวจากภัยพิบัติ (Disaster Recovery Plan)

2. วัตถุประสงค์

2.1 เพื่อสร้างความเข้าใจร่วมกันระหว่างผู้บริหารและผู้ปฏิบัติ ในการดูแลรักษาระบบความปลอดภัยฐานข้อมูลและสารสนเทศขององค์กร

2.2 เพื่อลดความเสียหายที่จะเกิดแก่ระบบเทคโนโลยีสารสนเทศ รวมถึงความเสียหายจากการไม่สามารถใช้ ระบบเทคโนโลยีสารสนเทศขององค์กร

2.3 เพื่อเป็นแนวทางในการดูแลรักษาระบบความมั่นคงปลอดภัยของฐานข้อมูลและสารสนเทศให้มีเสถียรภาพ และมีความพร้อมสำหรับการใช้งาน

2.4 เพื่อให้ระบบเทคโนโลยีสารสนเทศ สามารถดำเนินการได้อย่างต่อเนื่อง มี ประสิทธิภาพ สามารถแก้ไขสถานการณ์ได้อย่างทันท่วงที

2.5 เพื่อเตรียมความพร้อมรับสถานการณ์ฉุกเฉินที่อาจจะเกิดขึ้นกับระบบเทคโนโลยีสารสนเทศ

2.6 เพื่อให้เกิดความมั่นใจในความคงอยู่ของข้อมูลที่มีความสำคัญ เมื่อเกิดเหตุการณ์วิกฤต

3. เป้าหมาย

3.1 เพื่อลดความเสี่ยงและหลีกเลี่ยงความเสียหายแก่ทางราชการให้น้อยที่สุดเท่าที่จะทำได้

3.2 สร้างแผนปฏิบัติงานมาตรฐานสำหรับผู้ดูแลระบบ (Administrator)

3.3 ลดการตัดสินใจในช่วงเหตุการณ์วิกฤต

3.4 เพื่อให้ผู้ขอรับบริการสามารถใช้บริการทางด้านเทคโนโลยีสารสนเทศได้อย่างต่อเนื่อง

4. โครงสร้างทีมงานสำคัญ (Organization Chart)

ผู้บริหารระดับสูงต้องเห็นความสำคัญของการจัดทำแผนการกู้คืนความเสียหาย อีกทั้งสนับสนุนให้มีการพัฒนากระบวนการวางแผน การจัดระเบียบแผนการกู้คืนความเสียหาย ตลอดจนผลักดันทำให้มีการบรรลุผลการใช้งานระบบเทคโนโลยีสารสนเทศในองค์กร

คณะผู้บริหารแผนสถานการณ์ฉุกเฉินหรือภัยพิบัติ (Crisis Management Team) จะต้องประเมินความเสี่ยง และคำนึงถึงผลกระทบกับการดำเนินการขององค์กรที่เกี่ยวข้องกับความเสียหายที่อาจจะเกิดขึ้น ไม่ว่าจะเกิดจาก เหตุภัยธรรมชาติ ด้านเทคนิค หรือความผิดพลาดของมนุษย์ (Human Error) ตลอดจนวิเคราะห์และกำหนดความสำคัญตามความเป็นไปได้ตามความรับผิดชอบของทุกหน่วยงานย่อย รวมถึงการประเมินความเสี่ยงควรมีการประเมินผลความปลอดภัยด้วย

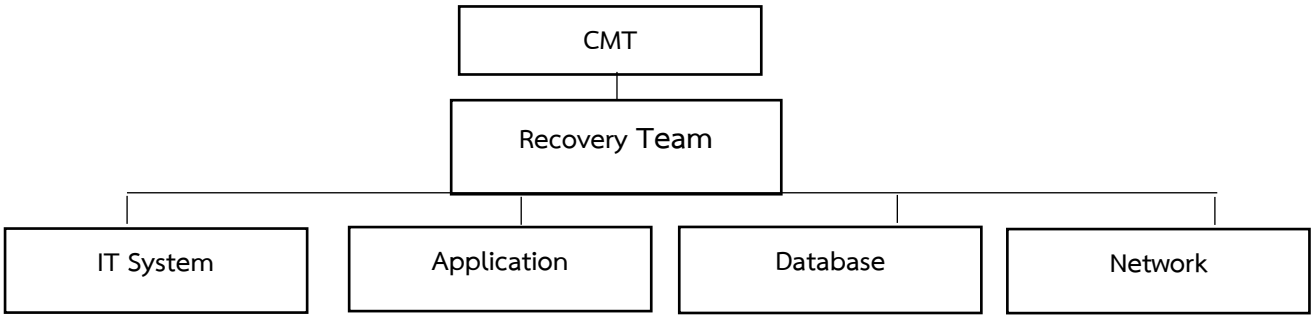
<u>การจัดองค์กรปฏิบัติการฉุกเฉินในระบบสารสนเทศเมื่อเกิดเหตุฉุกเฉิน</u>

4.1 ลำดับคณะผู้บริหารที่มีอำนาจสั่งการใช้แผนฉุกเฉิน เรียงตามลำดับ คือ

- ประธานเจ้าหน้าที่บริหาร
- รองประธานเจ้าหน้าที่บริหารด้านปฏิบัติการ
- ผู้จัดการฝ่ายเทคโนโลยีสารสนเทศ

4.2 โครงสร้างทีมงานกอบกู้ระบบ (DRP Organization Chart)

โครงสร้างทีมงานกอบกู้ระบบมีทีมย่อยภายใต้บังคับบัญชา 4 ทีม ดังนี้



- ทีมกอบกู้ส่วนวิศวกรระบบ (IT System Team)
- ทีมกอบกู้ส่วนโปรแกรมประยุกต์ (Application Team)
- ทีมกอบกู้ส่วนฐานข้อมูล (Database Team)
- ทีมกอบกู้ส่วนระบบเครือข่าย (Network Team)

5. ลำดับเหตุการณ์และขั้นตอนการปฏิบัติงาน

ลำดับ	ขั้นตอนการปฏิบัติงาน	รายละเอียด
1	เมื่อเหตุการณ์เกิดขึ้น	ให้ผู้ประสบเหตุการณ์แจ้งทีมงานกอบกู้ระบบโดยทันทีและ ดำเนินการยุติภัยที่เกิดโดยเร็ว
2	การประเมินความเสียหาย	ทีมงานประเมินสถานการและประเมินความเสียหายจากภัย ที่เกิดขึ้น
3	การตัดสินใจเริ่มใช้แผนกอบกู้	นำผลจากการประเมินสถานการและความเสียหายเพื่อตัดสิน ระบบงาน ใจและสั่งการให้ทีมผู้ที่เกี่ยวข้องปฏิบัติงานตามแผนกอบกู้ ระบบ
4	การปฏิบัติการกอบกู้	ดำเนินการปฏิบัติการกอบกู้ตามแผนและคู่มือที่กำหนดไว้
5	การกลับเข้าสู่ภาวะปกติ	ระบบคอมพิวเตอร์ของบริษัทฯสามารถใช้งานได้เป็น ปกติ

5.1. เมื่อเหตุการณ์เกิดขึ้น ในกรณีที่เกิดเหตุการณ์ฉุกเฉินขึ้น และจำเป็นต้องมีการอพยพออกจากตึก โดยขอให้เจ้าหน้าที่ปฏิบัติตามแผน อพยพ หรือแผนหนีไฟที่มีอยู่ ซึ่งจัดทำตามแผน BCP ทั้งนี้จำเป็นต้องปิดการทำงานของ ระบบคอมพิวเตอร์ (ถ้าสามารถทำได้ทัน) หรือหากเกิดภาวะร้ายแรง ไม่สามารถที่จะระบุสาเหตุที่ก่อให้เกิดความ ขัดข้องของระบบคอมพิวเตอร์เบื้องต้น แต่ในกรณีที่เกิดภาวะฉุกเฉินต่างๆ เช่น เพลิงไหม้ ภาวะฉุกเฉินจะถูก ประกาศใช้ทันที และต้องประสานงานตามแผน BCP

5.2. การประเมินความเสียหาย ทีมงานผู้รับผิดชอบแต่ละทีมจะทำการประเมินความเสียหายแล้วแต่กรณี โดยทำการตรวจสอบ ดังนี้

- ทำการตรวจสอบเครื่องคอมพิวเตอร์แม่ข่าย (Server Farms)
- ทำการตรวจสอบระบบเครือข่ายคอมพิวเตอร์และระบบสายสัญญาณสื่อสารฯ
- ทำการตรวจสอบ System Software
- ทำการตรวจสอบระบบ Firewall Anit-Spam
- ทำการตรวจสอบ Virus, Worm, Spy ware
- ทำการตรวจสอบ UPS และระบบไฟฟ้าฉุกเฉิน
- ทำการตรวจสอบระบบ Precision Air
- ทำการตรวจสอบ Transaction log files
- ทำการตรวจสอบการใช้งานข้อมูลระบบงานที่สำคัญ
- ทำการตรวจสอบระบบฐานข้อมูล

- ทำการตรวจสอบการเปลี่ยนแปลงของไฟล์ต่างๆ

- ทำการตรวจสอบความถูกต้องของไฟล์ข้อมูล

- ทำการตรวจสอบค่า Configuration ของระบบ

- ทำการตรวจสอบระบบสัญญาณจากผู้ให้บริการอินเตอร์เน็ตและอินทราเน็ต

- ทำการตรวจสอบทานบัญชีทรัพย์สิน รวมถึงมูลค่าความเสียหายของอุปกรณ์

- ทำการตรวจสอบอื่นๆ ที่เกี่ยวข้องระบบสารสนเทศ

5.3 การตัดสินใจเริ่มใช้แผนกอบกู้ การสรุปและประเมินสถานการณ์รายงานให้ผู้บริหารทราบ ซึ่งหากผลปรากฏว่า

<u>กรณีที่ระบบคอมพิวเตอร์ได้รับความเสียหายเพียงเล็กน้อยแต่ยังสามารถให้บริการได้ก็จะดำเนินการ</u>

1. เตรียมความพร้อมสำหรับการกอบกู้ข้อมูลจากระบบ Backup และ Media อื่นๆ

2. การเตรียมระบบคอมพิวเตอร์เปิดใช้งาน (หลังจากสำรวจสภาพความเสียหาย)

<u>กรณีที่ระบบคอมพิวเตอร์ของงานหลักได้รับความเสียหาย ไม่สามารถให้บริการได้ก็จะดำเนินการ</u>

1. ทำการ Start ระบบสำรองที่ DR Site เพื่อให้เจ้าหน้าที่สามารถใช้งานระบบงานที่มีความสำคัญ

2. การเตรียมความพร้อมสำหรับการกอบกู้ข้อมูลจากระบบ Backup และ Media อื่นๆ

3. จัดหาเครื่องคอมพิวเตอร์เพื่อนำมาทดแทนเครื่องคอมพิวเตอร์ตามแผน BCP

4. การเตรียมระบบคอมพิวเตอร์เปิดใช้งาน (หลังจากการ Restore และติดตั้งระบบ)

<u>กรณีที่ระบบคอมพิวเตอร์ได้รับความเสียหายมาก ไม่สามารถให้บริการได้ก็จะดำเนินการ</u>

1. การจัดหาสถานที่เพื่อย้ายระบบคอมพิวเตอร์ไปยังศูนย์คอมพิวเตอร์สำรอง

2. ทำการ Start ระบบสำรองที่ DR Site เพื่อให้เจ้าหน้าที่สามารถใช้งานระบบงานที่มีความสำคัญ

3. จัดหาเครื่องคอมพิวเตอร์ Server เพื่อนำมาทดแทนเครื่องคอมพิวเตอร์หลักที่เสียหาย โดยด่วน

4. การเตรียมความพร้อมสำหรับการกอบกู้ข้อมูลจากระบบ Backup และ ระบบบันทึกบน Media อื่นๆ

5. การเตรียมระบบคอมพิวเตอร์เปิดใช้งาน (หลังจากการ Restore และติดตั้งระบบ)

6. การเตรียมระบบเครือข่าย

7. ดำเนินการกอบกู้ระบบทำสำรองข้อมูล

5.4 การปฏิบัติการกอบกู้

หลังจากดำเนินการกอบกู้ข้อมูล โดยการ Restore ข้อมูลจาก Backup และ Media อื่นๆ เป็นที่เรียบร้อยแล้วทีมงานที่เกี่ยวข้องต้องดำเนินการใน Step ต่อไป ดังนี้

1. ระบบห้องเครื่องคอมพิวเตอร์แม่ข่าย เครื่องคอมพิวเตอร์แม่ข่าย อุปกรณ์รักษาความปลอดภัย อุปกรณ์เครือข่าย รวมถึง System Software & Utility จะถูกทดสอบความพร้อมก่อน

2. ระบบโปรแกรมประยุกต์ของบริษัทฯ จะถูกทดสอบเป็นระบบที่ 2 เพื่อดูความพร้อมและความถูกต้องก่อนที่จะเริ่มเปิดให้บริการ

3. เริ่มกระบวนการสำรองข้อมูลลงสู่ Backup และ Media อื่นๆ ชุดใหม่

4. ผู้ที่เกี่ยวข้องประกาศสถานการณ์และแจ้งการเปิดใช้งานระบบสารสนเทศ

5. หากมีทรัพย์สินที่ขนย้ายออกไปให้นำมาเก็บเข้าที่โดยต้องตรวจสภาพ และสอบทานบัญชีทรัพย์สิน ที่จัดทำและทำรายงานเสนอผู้บังคับบัญชาตามลำดับขั้น

5.5 การกลับเข้าสู่ภาวะปกติ

1. ใช้งานเครื่องคอมพิวเตอร์ Server ที่นำมาทดแทน แทนเครื่องคอมพิวเตอร์หลักที่เสียหาย

2. แผนการนำระบบคอมพิวเตอร์กลับสู่สภาพเดิม เพื่อให้สามารถใช้งานได้ตามปกติ (Return to Normal) โดยฝ่ายเทคโนโลยีสารสนเทศมีการกำหนดแผนเพื่อเปลี่ยนการใช้งานจากระบบคอมพิวเตอร์สำรองไปใช้ระบบคอมพิวเตอร์หลัก ณ ฝ่ายเทคโนโลยีสารสนเทศ โดยกำหนดแผนงาน การโอนย้ายกลับ ดังนี้

<u>แผนงานระยะสั้นภายใน 1-5 วัน</u>

- จัดเตรียมสิ่งอำนวยความสะดวก ตลอดจนอุปกรณ์ในการทำงานต่างๆ ตามแผน BCP ที่ได้กำหนดไว้

<u>แผนงานระยะกลางภายใน 1 เดือน</u>

- จัดหาอุปกรณ์การทำงานเพิ่มเติม เพื่อคืนสภาพในการดำเนินการของระบบงาน เช่น จัดหาเครื่องคอมพิวเตอร์Server หรือการปรับปรุงประสิทธิภาพและขยายความสามารถของเครื่องคอมพิวเตอร์ที่ฝ่ายเทคโนโลยีสารสนเทศ สำรองให้สามารถทำงานได้ใกล้เคียงกับความสามารถของเครื่องคอมพิวเตอร์ Server ปัจจุบัน

- ติดต่อประสานงานกับผู้ขายหรือตัวแทนจำหน่ายเพื่อจัดหาอุปกรณ์

แผนงานระยะยาวภายใน 3 เดือน

- จัดทำแผนในการกอบกู้ระบบงานขององค์กร เช่น การวางแผนในการจัดเตรียมศูนย์คอมพิวเตอร์ สำรอง หรือจัดหาสถานที่อื่นเพื่อจัดตั้งศูนย์คอมพิวเตอร์หลักที่เหมาะสมต่อไป

5.6 การจัดหาอุปกรณ์การทำงานต่างๆ เพิ่มเติม เพื่อคืนสภาพในการดำเนินงานขององค์กร

ขั้นตอนการโอนย้าย

- เตรียมข้อมูล ที่ได้ทำการ Back Up ไว้ มายัง DR Site เพื่อให้ผู้ใช้ระบบสามารถเปิดใช้งานข้อมูลที่เป็นข้อมูล Back Up ล่าสุด

- เตรียมระบบเครือข่าย เพื่อใช้ระบบที่ศูนย์เทคโนโลยีสารสนเทศประสานงาน ติดต่อ ผู้ให้บริการสัญญาณเครือข่าย เพื่อทราบและเชื่อมต่อวงจรทั้งระบบอินเตอร์เน็ต และระบบอินทราเน็ต

- เตรียมระบบอื่นที่เกี่ยวข้อง เพื่อทำการเปิดใช้งานระบบสารสนเทศเมื่อทำการสำรองข้อมูล กลับ (Synchronize Backward via Backup) ของข้อมูลที่มีการสำรองข้อมูลที่อยู่ ณ ฝ่ายเทคโนโลยีสารสนเทศเสร็จสิ้นแล้ว ระบบคอมพิวเตอร์หลักจะพร้อมเปิดให้บริการต่อ โดยปิดระบบงานที่ DR Site ซึ่งใช้เป็นระบบงานหลัก หลังจากเกิด Disaster

- เปิดระบบงานหลัก แทนระบบจาก DR Site

- เตรียมงาน เพื่อรองรับ Disaster ในอนาคต

6. กลยุทธ์การกอบกู้ระบบงาน (Recovery Strategy)

กลยุทธ์การกอบกู้ระบบงานเป็นกระบวนการหรือวิธีการที่ทำให้การกอบกู้ระบบงานประสบผลสำเร็จ สามารถแก้ไขสถานการณ์ที่ไม่พึงประสงค์ ซึ่งมีการกำหนดรายละเอียดและขอบเขตไว้ ดังนี้

6.1 กลยุทธ์ในการกอบกู้ระบบงานหลักที่สำคัญ

- บริษัทฯจะจัดหาสถานที่เพื่อใช้เป็นศูนย์ Wall room และ/หรือผู้ให้บริการ (IDC) ในการให้บริการระบบงานหลักชั่วคราว หากเกิดเหตุภัยพิบัติขึ้น และไม่สามารถดำเนินระบบงานต่อไปได้ ณ สาขาต่างๆ ตามแผน BCP

- เจ้าหน้าที่และผู้ใช้ระบบงานหลัก สามารถที่จะดำเนินงานต่อได้โดยใช้บริการของระบบคอมพิวเตอร์ ที่ DR Site

- ระบบงานต่างๆ ของ DR Site จะสามารถทำการเชื่อมต่อไปยัง หน่วยงานต่างๆ ที่จำเป็น เพื่อเปิดการให้บริการแทนต่อไปได้

- ระบบการทำสำรองข้อมูลระบบงานหลักจะใช้วิธี Backup สำหรับ เช่น Hard disk, DVD, CD-ROM สำหรับ Server ที่มี PLATFORM เป็น Windows Base

- ระบบงานหลักที่ให้บริการ มี ดังนี้

1) ระบบ SAPB1 , Plant One , Rental , Fix asset

2) ระบบ Intranet

3) ระบบ Sales Force

4) ระบบ Pay Roll

5) ระบบ File Server

6.2 การทำงานของระบบคอมพิวเตอร์สำรอง: ในกรณีเกิดเหตุภัยพิบัติ (Disaster)

- เตรียมข้อมูลสำรอง เพื่อทำการเปิดใช้งาน ณ DR Site ข้อมูลสำรองที่มี จัดเก็บ ณ ตู้นิรภัยฝ่ายเทคโนโลยีสารสนเทศ จำนวน 1 ชุด และฝากจัดเก็บ ณ ผู้ช่วยผู้จัดการ จำนวน 1 ชุดได้แก่ ข้อมูลที่ทำ สำรองบนระบบ Backup เช่น Hard disk, DVD, CD-ROM สำหรับ Server ที่มีPLAT FORM เป็น Windows Base ดังนั้นการกอบกู้กลับจะใช้ข้อมูลจากBackup และ Media ดังกล่าว

- จัดหาเครื่องคอมพิวเตอร์และอุปกรณ์ต่อพ่วงที่จำเป็น

- การเตรียมความพร้อมสำหรับการกอบกู้ข้อมูลจากระบบ Backup และ Media อื่นๆ

- เตรียมระบบเครือข่าย เพื่อใช้งานระบบ ในกรณีที่ระบบเครือข่ายเกิดความเสียหาย

- เปิดระบบงานหลัก

1) เปิดระบบปฏิบัติการโดยใช้ข้อมูลที่เตรียมข้างต้น

2) เปิดระบบงานหลัก เพื่อให้บริการตามปกติ

เมื่อระบบคอมพิวเตอร์หลักสามารถใช้งานได้ตามปกติ (Return to Normal) ควรมีการวางแผนเพื่อเปลี่ยนการใช้งานที่ระบบคอมพิวเตอร์สำรองไปใช้ระบบคอมพิวเตอร์หลัก ขั้นตอน การโอนย้ายกลับมีดังนี้

- เตรียมข้อมูล ที่ DR Site เพื่อการโอนย้ายกลับ ข้อมูลที่อยู่ DR Site คอมพิวเตอร์สำรองซึ่งเปิดใช้เป็นระบบข้อมูลหลัก จะต้องถูกถ่ายโอนกลับมายัง Server หลักเพื่อให้ผู้ใช้ระบบงานสามารถ เปิดใช้งานด้วยข้อมูลที่เป็นปัจจุบัน

- เตรียมระบบเครือข่าย เพื่อใช้ระบบที่ศูนย์เทคโนโลยีสารสนเทศ

- เตรียมระบบ เพื่อทำการเปิดใช้งานศูนย์เทคโนโลยีสารสนเทศ เมื่อทำการสำรองข้อมูลกลับ (Synchronize Backward via Backup) ของข้อมูลที่มีอยู่ DR Site และข้อมูลที่อยู่ Server หลักเสร็จสิ้นแล้ว ระบบคอมพิวเตอร์หลักจะพร้อมเปิดให้บริการต่อ โดยปิดระบบงานที่ DR Site ซึ่งใช้เป็นระบบงานหลัก หลังจากเกิด Disaster

- เปิดระบบงานหลัก แทนระบบจาก DR Site

- เตรียมงาน เพื่อรองรับ Disaster ในอนาคต

7. ความหมายและประเภทของภาวะฉุกเฉินหรือภัยพิบัติ

ภาวะฉุกเฉิน (Emergencies) เป็นสภาวะที่ไม่เป็นปกติของสิ่งแวดล้อมซึ่งอาจเกิดจากการเปลี่ยนแปลงตามธรรมชาติหรือจากการกระทำของมนุษย์ อันจะก่อให้เกิดผลกระทบทางลบ และความเสียหายต่อระบบเทคโนโลยี สารสนเทศขององค์กรรวมถึงสิ่งแวดล้อมเองและสุขภาพอนามัยของบุคลากรได้ ภาวะฉุกเฉินอาจเกิดขึ้นได้อย่าง เฉียบพลัน มีผลกระทบในระยะสั้นๆ หรืออาจเกิดสะสมมาเป็นระยะเวลาหนึ่ง และมีผลกระทบอย่างต่อเนื่อง ยาวนานก็ได้ ทั้งนี้ ขึ้นอยู่กับ รูปแบบและลักษณะของความผิดปกติที่เกิดขึ้นนั้นๆ ประเภทของภาวะฉุกเฉิน ภาวะ ฉุกเฉินแบ่งตามลักษณะของสาธารณภัยภัยหรือความผิดปกติของสิ่งแวดล้อมที่เกิดขึ้น ดังนี้

7.1 ภาวะฉุกเฉินจากภัยธรรมชาติ (Natural Disaster) เป็นภาวะฉุกเฉินที่เกิดจากภัยที่เกิดขึ้นเองตาม ธรรมชาติ มักเกิดขึ้นตามฤดูกาลเป็นส่วนใหญ่แต่บางครั้งก็เกิดขึ้นโดยไม่รู้ตัว ซึ่งสามารถก่อให้เกิดความเสียหายแก่ระบบเทคโนโลยีสารสนเทศ รวมถึงชีวิตและทรัพย์สินเป็นอย่างมาก ภาวะฉุกเฉินจากภัยธรรมชาติ สามารถแยกย่อย ได้อีก ดังนี้

- สาธารณภัยเชิงอุตุนิยมวิทยา (meteorological disaster) เกิดขึ้นตามฤดูกาล คือ วาตภัย ภัยที่เกิดจากแรงลมและพายุ เช่นพายุดีเปรสชั่น พายุโซนร้อน พายุไต้ฝุ่น พายุไต้ฝุ่นที่มีอำนาจทำลายสูงมาก สามารถทำให้ ต้นไม้ถอนรากถอนโคน อากาศหนาวผิดปกติเช่น ในภาคเหนือและตะวันออกเฉียงเหนือของประเทศอุณหภูมิใน บางปีลดต่ำลงใกล้ศูนย์องศาเซลเซียส คลื่นความร้อน (heat wave) ทำให้อากาศร้อนผิดปกติในประเทศเขตหนาวทำ ให้ผู้ป่วยโรคหัวใจเสียชีวิตมากขึ้น ฝนแล้ง (drought) ทำให้ข้าวและพืชผลทางการเกษตรเสียหายมาก เกิดความขาด แคลนและอดอยาก เป็นต้นเหตุของทุพภิกขภัยอย่างหนึ่ง

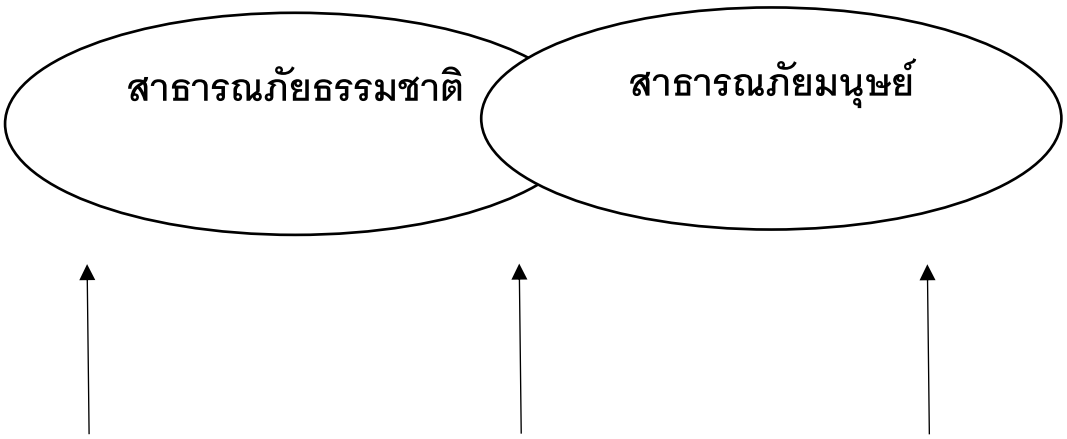
- สาธารณภัยตามสภาพภูมิประเทศ (topological disaster) เป็นสาธารณภัยที่เกิดขึ้นตามลักษณะของ ภูมิประเทศ สาธารณภัยประเภทนี้ได้แก่ อุทกภัย ภัยอันเกิดจากน้ำท่วม ประเทศไทยประสบปัญหาน้ำท่วมเกือบทุกปี ปีเนื่องจากมีการตัดไม้ ทำลายป่า การทรุดตัวของดิน มีลมพายุและลมมรสุมรุนแรง ฝนตกหนักและน้ำทะเลหนุน หิมะถล่ม ซึ่งถ้าไม่มีอันตรายต่อชีวิตและทรัพย์สิน ไม่จัดเป็นสาธารณภัย

- สาธารณภัยที่เกิดจากการเปลี่ยนแปลงพื้นผิวโลก(tectonic disaster) การเปลี่ยนแปลงของผิวโลกทำ ให้เกิดแผ่นดินเลื่อน แผ่นดินไหว ภูเขาไฟระเบิด เป็นต้น แผ่นดินเลื่อนหรือแผ่นดินถล่ม (landslide) การ

เปลี่ยน ระดับของชั้นผิวโลกทำให้เกิดการไหวและสั่นสะเทือนของอาคารบ้านเรือน บางครั้งเมื่อมีฝนตกหนัก ไม่มีการยึด เหนี่ยวของพื้นผิวดิน อาจทำให้พื้นผิวดินพังทลายลงมาและเป็นอันตรายได้ แผ่นดินไหว (earthquake) คือ การเปลี่ยนแปลงของผิวโลกที่มีการสั่นสะเทือนเป็นลูกคลื่นและเป็นระลอกเคลื่อนจากจุดศูนย์กลางออกไป ทุกทิศทาง ทำลายบ้านเรือนและ สิ่งก่อสร้างต่างๆ ภูเขาไฟระเบิด (volcanic eruption) เป็นการปลดปล่อยหินละลาย และแร่ธาตุต่างๆ จากใต้พื้นผิวโลกออกมาซึ่งบางครั้งก็อาจเป็นเพียงขี้เถ้า หรือควันดำ หรืออาจเป็นหินหลอมเหลวที่ มีความร้อนสูงอันเป็นอันตรายต่อชีวิตและทรัพย์สิน

- สาธารณภัยทางชีวภาพ (biological disaster) เป็นสาธารณภัยที่มีสาเหตุเนื่องมาจากสิ่งมีชีวิต เช่น เชื้อโรคต่างๆ ที่ทำให้เกิดโรคระบาด สัตว์และแมลงที่ทำลายพืชไร่ทางเกษตรกรรม การระบาดของโรค เช่น อหิวาตกโรค กาฬโรค โปลิโอ ไข้สมองอักเสบ เป็นต้น โรคติดต่อต่างๆ สามารถทำให้เกิดการระบาดของโรคได้ใน เมื่อมีแหล่งแพร่เชื้อที่เหมาะสม มีการแพร่กระจายของโรค และภูมิคุ้มกันของกลุ่มชนต่ำ ภัยจากฝูงสัตว์และแมลง เกิดจากสัตว์บางชนิด เช่น หนูนา ตั๊กแตน ฯลฯ ที่ทำลายพืชผลทางการเกษตรได้ อันนำมาซึ่งการเกิดทุพภิกขภัยหรือ การระบาดของโรคจากอาหารได้

7.2 ภาวะฉุกเฉินจากภัยมนุษย์ (Man-made disaster) เป็นภาวะฉุกเฉินที่เกิดจากการกระทำของมนุษย์ทั้ง โดยความไม่ตั้งใจ ประมาท เผลอเรอ และความตั้งใจในการทำลายล้างหรือกลั่นแกล้งซึ่งกันและกัน ได้แก่ ภัยจากการจราจร ทั้งทางอากาศ ทางบก ทางน้ำ ภัยจากการอุตสาหกรรม เช่น การระเบิดของเครื่องจักร ภัยจากการก่อสร้าง เช่น อุบัติเหตุจากการก่อสร้าง ภัยจากการขัดแย้งในผลประโยชน์หรือการก่ออาชญากรรมในที่สาธารณะ เช่น การก่อการทะเลาะวิวาท ภัยจากการก่อวินาศกรรม เช่น การลอบวางระเบิด ลอบสังหารบุคคลต่างๆ ภัยจากการจลาจล เช่น การประท้วงรัฐบาล การก่อความไม่สงบภายในประเทศ ภัยจากการรวมกลุ่มของบุคคลคณะใด คณะหนึ่งกระทำการมิชอบด้วยกฎหมาย ด้วยความตั้งใจและใช้ความรุนแรง เพื่อให้บรรลุวัตถุประสงค์ทำให้เกิด ภยันตรายขึ้นได้ ภัยจากสงคราม เช่น สงครามโลก สงครามเกาหลี สงครามเวียดนาม อย่างไรก็ตาม ภาวะฉุกเฉินทั้งสองประเภทนี้อาจมีที่มาที่แตกต่างกัน แต่ก็มักจะก่อให้เกิดภัยพิบัติใน ลักษณะเดียวกันได้ เช่น ทั้งภัยธรรมชาติและภัยจากมนุษย์ก็สามารถก่อให้เกิด ไฟไหม้ อาคารก่อสร้างถล่ม การ ระบาดของโรคได้ เป็นต้น จากสาธารณภัยที่ก่อให้เกิดภาวะฉุกเฉินมาทั้งหมดนี้ อาจนำมาสรุปความสัมพันธ์ตาม แผนภาพ ดังนี้



- วาตภัย
- อากาศหนาวผิดปกติ
- คลื่นความร้อน
- ฝนแล้ง
- อุทกภัย
- หิมะถล่ม
- แผ่นดินเลื่อน
- ภูเขาไฟระเบิด

- อัคคีภัย
- ไฟไหม้ป่า
- อุทกภัย
- การระบาดของโรค

- ภัยจากการจราจร
- ภัยจากการอุตสาหกรรม
- ภัยจากการก่อสร้าง
- ภัยจากการขัดแย้งในผลประโยชน์
- ภัยจากการก่อวินาศกรรม
- ภัยจากจลาจล
- ภัยจากสงคราม
- อัคคีภัย การวางเพลิง

8. การประเมินสถานการณ์ความเสี่ยงแนวโน้มภัยที่อาจเกิดขึ้นกับระบบเทคโนโลยีสารสนเทศ

จากการศึกษาวิเคราะห์ ติดตามตรวจสอบและประเมินสถานการณ์ความเสี่ยงจากภัยต่างๆ ในปีปัจจุบันที่จะกระทบต่อระบบเทคโนโลยีสารสนเทศ พบว่าความเสี่ยงที่เป็นอันตราย (disaster) และมี โอกาสเกิดขึ้นต่อระบบเทคโนโลยีสารสนเทศได้มากที่สุด สามารถกำหนดและสรุปแบ่งประเภท ภัยได้ 4 ข้อ ดังนี้

1 ภัยที่เกิดจากเจ้าหน้าที่หรือบุคลากรของหน่วยงาน (Human error) ทั้งโดยเจตนาหรือไม่เจตนา

2 ภัยที่เกิดจากบุคคลภายนอกหน่วยงาน ทั้งโดยเจตนาหรือไม่เจตนา

3 ภัยที่เกิด Software ที่ไม่พึงประสงค์

4 ภัยจากไฟไหม้หรือ จากระบบไฟฟ้า

8.1 ภัยที่เกิดจากเจ้าหน้าที่หรือบุคลากรของหน่วยงาน (Human error) ทั้งโดยเจตนาหรือไม่เจตนา ได้แก่ กรณีเจ้าหน้าที่หรือบุคลากรของหน่วยงานขาดความรู้ความเข้าใจในเครื่องมืออุปกรณ์คอมพิวเตอร์ทั้งด้าน Hardware Software และระบบโปรแกรมประยุกต์รวมถึงความรู้และการตระหนักในเรื่องของการรักษาความปลอดภัยทางด้านเทคโนโลยีสารสนเทศ ซึ่งอาจส่งผลทำให้ระบบเทคโนโลยีสารสนเทศเสียหาย ใช้งานไม่ได้ เกิดการชะงัก งันรบกวน หยุดทำงาน หรือไม่สามารถใช้งานระบบเทคโนโลยีสารสนเทศได้อย่างเต็มประสิทธิภาพ และ/หรือเกิด จากเจตนาที่ไม่ดีของผู้ดูแลระบบ (Administrator) และ/หรือ ผู้ที่มีอำนาจในการเข้าถึงอุปกรณ์หรือเข้าถึงระบบที่ไม่ พึงพอใจการบริหารงานทรัพยากรบุคคล สภาพการปฏิบัติงานขาดขวัญและกำลังใจ การเจตนากลั่นแกล้งหรือมีเป้าประสงค์ทำให้ระบบเทคโนโลยีสารสนเทศหยุดให้บริการ

8.2 ภัยที่เกิดจากบุคคลภายนอกหน่วยงาน ทั้งโดยเจตนาหรือไม่เจตนา ได้แก่ ผู้ที่จะพยายามจะโจมตีระบบคอมพิวเตอร์ โดยขึ้นอยู่กับแรงจูงใจที่จะกระทำและเครื่องมือที่ใช้กระทำมีตั้งแต่เครื่องมือพื้นฐาน ไปจนถึงเครื่องมือที่ซับซ้อนและมีอำนาจการทำลายสูง ซึ่งส่งผลทำให้ระบบเทคโนโลยีสารสนเทศเสียหาย ใช้งาน ไม่ได้ เกิดการชะงักงันหยุดทำงาน หรือไม่สามารถใช้งานระบบเทคโนโลยีสารสนเทศได้อย่างเต็มประสิทธิภาพ ซึ่งสามารถแยกประเภทของผู้บุกรุกหรือนักโจมตีระบบหรือนักเจาะระบบได้ ดังนี้

ผู้บุกรุก	ระดับความสามารถ	แรงจูงใจ
แฮคเกอร์ (Hacker)	สูง	เพื่อปรับปรุงระบบรักษาความปลอดภัย
แครกเกอร์ (Cracker)	สูง	เพื่อทำลายระบบ
สคริปคิดดี้ (Scriptkiddy)	สูง	เพื่อให้ได้การยอมรับ
สายลับ (Spy)	สูง	เพื่อให้ได้เงิน
ผู้ก่อการร้าย(Terrorist)	สูง	เพื่ออุดมการณ์

แนวทางปฏิบัติเพื่อเตรียมรับสถานการณ์ภัยจากบุคคลภายนอก

ภัยคุกคามจากบุคคลภายนอกนับเป็นภัยที่สำคัญที่ทุกองค์กรได้ให้ความสำคัญ และระมัดระวัง ในเรื่องของการรักษาความปลอดภัยมากที่สุดไม่ว่าจะเป็นการรักษาความปลอดภัยทางด้านกายภาพ (Physical) และการรักษาความปลอดภัยทางด้านตรรก (Logical) ซึ่งเอกสารนี้ได้กำหนดแนวทางการดำเนินการเบื้องต้นเพื่อลดปัญหาความเสี่ยงที่จะเกิดขึ้นกับระบบเทคโนโลยีสารสนเทศไว้โดยแบ่งเป็น 5 ช่วงระยะ ดังนี้ ระยะเวลาการป้องกันและเตือนภัยเพื่อเตรียมรับสถานการณ์ การมีระบบป้องกันและเตือนภัยว่ามีบุคคลแปลกปลอมได้บุกรุกระบบคอมพิวเตอร์ ขององค์กร ให้กับผู้ดูแล ระบบ (Administrator) ทราบล่วงนับว่ามีความสำคัญและจำเป็นอย่างยิ่ง เพื่อที่ผู้ดูแลระบบจะได้เตรียมการปฏิบัติ อย่างถูกต้องตามหลักวิชาและตามขั้นตอนที่กำหนดไว้ อันจะมีผลให้เกิดความเสียหายหรือความสูญเสียเกิดขึ้นน้อย ที่สุด โดยมีขั้นตอนดำเนินการ ดังนี้

1. การกำหนดให้มีการสำรวจ ติดตามตรวจสอบ และวิเคราะห์ระบบคอมพิวเตอร์และระบบเครือข่ายเพื่อหาช่องโหว่ควบคู่ไปกับการป้องกันขององค์กรทุก 1 เดือนโดยตรวจหาพื้นที่แต่ละจุดที่สามารถเชื่อมต่อเข้าเครือข่าย อินเตอร์เน็ตได้ การให้บริการและการใช้งาน และวิธีการควบคุม วิธีการป้องกันอุปกรณ์ต่างๆ การกำหนดนโยบาย ไฟร์วอล รวมถึงการใช้ซอฟต์แวร์ที่สามารถสแกนเครือข่ายเพื่อตรวจสอบ

2. การรักษาความปลอดภัยทางด้านกายภาพ (Physical Securities) มีการเข้าถึงโดยการสแกนลายนิ้วมือตลอด 24 ชั่วโมง รวมถึงประตูทางเข้าห้องทำงานจะต้องมี การเบิกจ่ายกุญแจ และมีบัตรอนุญาต (Proximity Card) จึงจะผ่านประตูได้

3. ขอรับงบประมาณสนับสนุนในการจัดซื้อจัดหาอุปกรณ์และการพัฒนาบุคลากรเพื่อเข้ารับการอบรมหลักสูตรเกี่ยวกับการป้องกันและรักษาความปลอดภัยทางด้านสารสนเทศในระดับผู้ดูแลระบบ (Administrator) เพื่อ เรียนรู้รูปแบบและวิธีการป้องกัน การโจมตีระบบคอมพิวเตอร์ รูปแบบต่างๆ

4. มีการติดตั้งอุปกรณ์ Internal & External firewall ซึ่งเป็นอุปกรณ์ ติดตั้งอยู่ที่ห้องคอมพิวเตอร์แม่ข่าย ทำ หน้าที่ในการกำหนดสิทธิการเข้าใช้งานเครื่องคอมพิวเตอร์แม่ข่ายและป้องกันการบุกรุกของ บุคคลจากทั้งภายใน และจากภายนอก

8.3 ภัยที่เกิดจาก Software ที่ไม่พึงประสงค์ ภัยนี้สามารถสร้างความเสียหายหรือการรบกวนการใช้งานแก่ ระบบคอมพิวเตอร์ อุปกรณ์คอมพิวเตอร์หรือระบบเครือข่าย ภัยดังกล่าวนี้ประกอบด้วย ไวรัสคอมพิวเตอร์ (Computer Virus) หนอนอินเตอร์เน็ต (Internet Worm) ม้าโทรจัน (Trojan Horse) และข่าวไวรัสหลอกลวง (Hoax) เป็นต้น พวก Software เหล่านี้มีผลกระทบต่อการทำงาน และก่อให้เกิดความเสียหายให้แก่ระบบเทคโนโลยี สารสนเทศ ถึงขั้นทำให้ระบบเครือข่ายคอมพิวเตอร์ล่ม และใช้งานไม่ได้

แนวทางปฏิบัติเพื่อเตรียมรับสถานการณ์ภัยจาก Software ที่ไม่พึงประสงค์

ภัยคุกคามจากซอฟต์แวร์ที่ไม่พึงประสงค์เป็นภัยที่มีความถี่ของการเกิดภัยและอันตรายมากที่สุด ซึ่งจะทำลาย ข้อมูล หรือ ทำลายระบบ หรือรบกวนการทำงาน ในการใช้ระบบอุปกรณ์ และที่มาของภัยนี้ส่วนใหญ่เกิดจากการ ขาดความระมัดระวังและจิตสำนึกในการใช้ระบบเทคโนโลยีสารสนเทศของคนในองค์กร เอกสารฉบับนี้ได้กำหนด แนวทางการดำเนินการเบื้องต้นเพื่อลดปัญหาความเสี่ยงที่จะเกิดภัยดังกล่าวไว้โดยแบ่งเป็น 5 ช่วงระยะ ดังนี้

ระยะเวลาการป้องกันและเตือนภัยเพื่อเตรียมรับสถานการณ์ การมีระบบป้องกันและเตือนภัยให้ผู้ดูแลระบบ (Administrator) และ/หรือผู้ใช้ระบบสารสนเทศทราบ เพื่อที่จะได้มีการเตรียมปฏิบัติหรือแก้ไขได้อย่างถูกต้องตามหลักวิชาและตามขั้นตอนที่กำหนด ไว้ รวมถึงการกำหนดมาตรการระเบียบ รวมถึงข้อบังคับในอันที่จะบังคับให้ผู้ใช้ระบบเทคโนโลยีสารสนเทศ เกิดจิตสำนัก ความตระหนัก ระมัดระวังการใช้งานและขั้นตอนการปฏิบัติอันจะมีผลให้ลดความเสียหายหรือความ สูญเสียต่อองค์กรเกิดขึ้นน้อยที่สุด จึงเห็นควรกำหนดวิธีการ ต่อไปนี้

1. มีการจัดหาและติดตั้งอุปกรณ์ Anti-Spam รวมถึงติดตั้งซอฟต์แวร์ Anti-virus ที่เครื่องให้บริการ (Server) และเครื่องลูกข่าย (Client) เพื่อทำหน้าที่ดักจับไวรัสที่เข้ามาในระบบคอมพิวเตอร์และระบบเครือข่าย และสามารถ ตรวจสอบได้ว่า มีไวรัสชนิดใดเข้ามาทำความเสียหายกับระบบคอมพิวเตอร์และระบบเครือข่ายคอมพิวเตอร์

2. แจ้งข้อมูลเตือนภัยไวรัสคอมพิวเตอร์ผ่านทางระบบอินทราเน็ตที่ 192.168.1.6 อย่าง ต่อเนื่องสม่ำเสมอ รวมทั้งแนะนำวิธีการป้องกันและการกำจัดภัยที่จะเกิดจาก Software ดังกล่าว ให้เจ้าหน้าที่ได้ ศึกษาและสามารถปฏิบัติการป้องกันและแก้ไขปัญหา

3. วางกฎระเบียบให้เจ้าหน้าที่ปฏิบัติ ตามระเบียบ IT Policy ว่าด้วยการรักษาความปลอดภัยในการใช้งานระบบคอมพิวเตอร์ เรื่อง นโยบายการรักษาความปลอดภัย ระบบเทคโนโลยีสารสนเทศ ลงวันที่ 1 เมษายน พ.ศ. 2563 และ เรื่อง มาตรการรักษาความปลอดภัยระบบเทคโนโลยีสารสนเทศสำหรับบุคคลภายนอกที่ไม่ใช่เจ้าหน้าที่ ลงวันที่ 1 เมษายน พ.ศ. 2563 ทั้งนี้ ได้ประชาสัมพันธ์แจ้งเวียนระเบียบดังกล่าวให้ทุกหน่วยงานทราบและถือปฏิบัติ รวมทั้งประกาศในระบบอินทราเน็ต

4. จัดจ้างบริษัทที่มีบุคลากรซึ่งมีความรู้ความชำนาญ ทำหน้าที่ดูแล ให้คำปรึกษา ตรวจสอบและบำรุงรักษา ระบบเครือข่ายไมโครคอมพิวเตอร์ทั้งทางด้าน Hardware และ Software โดยมีเจ้าหน้าที่ผู้ชำนาญการร่วมปฏิบัติงานกับส่วนเทคโนโลยีคอมพิวเตอร์และ การสื่อสารข้อมูล เป็นประจำทุกวันทำการและ/หรือวันหยุดราชการตลอด 24 ชั่วโมง

8.4 ภัยจากไฟไหม้ หรือ จากระบบไฟฟ้า จัดเป็นภัยร้ายแรงที่ทำความเสียหายให้แก่ระบบเทคโนโลยี สารสนเทศ ซึ่งบริษัทฯ ได้ให้ความสำคัญและระมัดระวังเป็นอย่างยิ่งที่จะไม่ให้เกิดภัยลักษณะดังกล่าวขึ้น

<u>แนวทางปฏิบัติเพื่อเตรียมรับสถานการณ์ภัยจากไฟไหม้หรือระบบไฟฟ้าขัดข้อง</u>

การเกิดสถานการณ์ไฟไหม้ อาจเกิดจากภัยจากมนุษย์หรืออุบัติเหตุก็ได้ซึ่งผลเสียหายขึ้นอยู่กับการป้องกันและการระงับภัยในทันท่วงทีซึ่งหากสามารถควบคุมได้ทันเวลาระยะเวลาการฟื้นฟูหรือกู้ภัยดังกล่าวก็จะใช้เวลา สั้น

ลง สำหรับระบบไฟฟ้าขัดข้องสถานการณ์ดังกล่าวโอกาสเกิดมีจำนวนครั้งไม่มากนักดังนั้นการเตรียมการ ป้องกันไว้จึงเป็นสิ่งที่ดี

<u>ระยะเวลาการป้องกันและเตือนภัยเพื่อเตรียมรับสถานการณ์</u>

บริษัทฯ ได้ตระหนักถึงปัญหาดังกล่าวที่อาจจะเกิดขึ้น จึงได้ดำเนินการ ดังนี้

1. ติดตั้งอุปกรณ์สำรองไฟฟ้า (UPS) ขนาด 6 KVA จำนวน 1 ชุด เพื่อควบคุมการจ่ายกระแสไฟฟ้าให้กับระบบเครื่องแม่ข่าย (Server) ในกรณีเกิดกระแสไฟฟ้าขัดข้อง ซึ่งระบบสำรองไฟฟ้าที่ใช้ควบคุมระบบคอมพิวเตอร์ และอุปกรณ์เครือข่าย ซึ่งสามารถสำรองไฟฟ้าเพื่อใช้งานได้นานประมาณ 30 นาที ถึง 1 ชั่วโมงในกรณีที่เกิดกระแสไฟฟ้าขัดข้องโดยระบบคอมพิวเตอร์และระบบเครือข่ายคอมพิวเตอร์จะสามารถให้บริการได้ในระยะเวลาที่สามารถ จัดเก็บและสำรองข้อมูลไว้อย่างปลอดภัย

2. ติดตั้งอุปกรณ์ตรวจจับควัน กรณีที่เกิดเหตุการณ์กระแสไฟฟ้าขัดข้องหรือมีควันไฟเกิดขึ้นภายในห้องควบคุมระบบเครือข่าย อุปกรณ์ดังกล่าวจะส่งสัญญาณแจ้งเตือนไปยังผู้ดูแลระบบ ผ่านแอพพลิเคชั่น (Promtec Plus) เพื่อทราบ และรีบ เข้ามาระงับเหตุฉุกเฉินอย่างทันท่วงที ซึ่งมีการตรวจสอบความพร้อมของอุปกรณ์อย่างสม่ำเสมอ

3. ติดตั้งอุปกรณ์ดับเพลิงชนิดก๊าซ ที่ห้องควบคุมระบบคอมพิวเตอร์เพื่อไว้ใช้ในกรณีเหตุฉุกเฉิน (ไฟไหม้) โดยมีการตรวจสอบความพร้อมของอุปกรณ์และทดสอบการใช้งานอย่างน้อยปีละ 1 ครั้ง

System Description

Physical Environment

ปัจจุบันบริษัทฯ ได้จัดหาระบบรักษาความปลอดภัยสำหรับการป้องระบบสารสนเทศจากเหตุต่างๆ ที่ อาจเกิดขึ้นได้ เช่น

ระบบเครื่องสำรองไฟฟ้าอัตโนมัติ (UPS System)

CLEANLINE UPS รุ่น T-6000

มีการติดตั้งระบบ UPS ขนาด 6 KVA จำนวน 1 ชุด ซึ่งสามารถสำรองไฟฟ้าให้กับ ระบบคอมพิวเตอร์ของบริษัทฯ ที่ติดตั้ง ณ ห้อง Server ชั้น 4 ได้อย่างมี ประสิทธิภาพ ระบบปรับอากาศแบบควบคุมความชื้น (Precision Air Conditioning System) มีการติดตั้งระบบปรับอากาศแบบควบคุมความชื้น (Precision Air Conditioning System) ขนาด 12,000 BTU จำนวน 2 เครื่อง สำหรับรองรับการทำงานของระบบคอมพิวเตอร์ของบริษัทฯ โดยได้มีการติดตั้งระบบ เครื่องปรับอากาศนี้ ณ ห้องเครื่องคอมพิวเตอร์ (Server Room) และด้วยความสามารถในการปรับลดอุณหภูมิและ ความชื้นได้อย่างมีประสิทธิภาพ ทำให้ระบบคอมพิวเตอร์สามารถทำงานได้อย่างมีเสถียรภาพ

ระบบควบคุมการเข้า –ออก อัตโนมัติ (Access Control System)

Hip C 809

ควบคุมการเข้า –ออก โดยใช้ Finger Scan มีการติดตั้งระบบควบคุมการเข้า–ออก อัตโนมัติ (Access Control System) เพื่อควบคุมการเข้า–ออก ของเจ้าหน้าที่ รวมถึงบุคคลภายนอก ที่จะเข้ามาภายในศูนย์สารสนเทศ และห้องต่างๆ ที่มีการควบคุมในเรื่องของ การรักษาความปลอดภัย (Security)

9. บทบาทหน้าที่และความรับผิดชอบของทีมงาน (Team Role & Responsibilities)

การเตรียมความพร้อมเพื่อรองรับเหตุการณ์ฉุกเฉินที่เกิดขึ้นจะมีการจัดแบ่งหน้าที่ความรับผิดชอบออกเป็น 2 ส่วน ดังนี้

9.1 ทีมงานคณะผู้บริหารในสถานการณ์ฉุกเฉินหรือภัยพิบัติ (Crisis Management Team) ประกอบด้วยกลุ่มของคณะผู้บริหารโดยมีหน้าที่หลัก ดังนี้

- ประเมินสถานการณ์ ควบคุม สั่งการรวมถึงการประกาศภาวะฉุกเฉินและยกเลิกภาวะฉุกเฉิน
- มีอำนาจอนุมัติค่าใช้จ่ายและอื่นๆ ที่เกิดขึ้นระหว่างภาวะฉุกเฉิน
- มอบหมายและ/หรือ แถลงข่าว ประชาสัมพันธ์ ให้สัมภาษณ์และเผยแพร่ข้อมูลแก่เจ้าหน้าที่ ของบริษัทและสาธารณชน เป็นต้น (ถ้ามี)

9.2 ทีมงานปฏิบัติการกอบกู้ในสถานการณ์ฉุกเฉินหรือภัยพิบัติ (Crisis Operation Team) ประกอบด้วย 4 ทีมงานย่อยซึ่งมีหน้าที่หลักในการดำเนินกระบวนงานกอบกู้ระบบตามแผนการกอบกู้ระบบ คอมพิวเตอร์ให้กลับสู่สภาพปกติในระยะเวลาอันสั้นที่สุด โดยแบ่งหน้าที่รับผิดชอบของแต่ละทีมงานย่อย ดังนี้

9.2.1 ทีมกอบกู้ส่วนวิศวกรระบบ (IT System Team)

- จัดเตรียมการในส่วนที่เกี่ยวข้องเพื่อให้ระบบสารสนเทศสามารถดำเนินงานต่อไปได้
- รับผิดชอบในการกอบกู้ระบบคอมพิวเตอร์และอุปกรณ์เครือข่ายและการเชื่อมต่อ กับระบบภายนอก

- ติดต่อประสานงานกับหน่วยงานที่เกี่ยวข้องเพื่อขอการสนับสนุนและให้คำปรึกษา เกี่ยวกับการติดตั้งและใช้งานระบบเทคโนโลยีสารสนเทศ

- รับผิดชอบในการกอบกู้ระบบงานต่างๆ ให้พร้อมใช้งานในเวลาที่กำหนด

- การพิจารณาและนำเสนอความคืบหน้าการกอบกู้ของแต่ละระบบให้ทราบ

9.2.2 ทีมกอบกู้ส่วนโปรแกรมประยุกต์ (Application Team)

- จัดเตรียมการย้ายส่วนประมวลผลของระบบโปรแกรมประยุกต์ ให้สามารถ ดำเนินงานต่อได้

- รับผิดชอบในการกอบกู้ระบบงานหลักที่สำคัญ (โปรแกรมประยุกต์ต่างๆ)

- ติดต่อและประสานงานไปยังหน่วยงานที่เกี่ยวข้องเพื่อขอการสนับสนุนและให้คำปรึกษา

- ประสานงานในการกอบกู้ระบบคอมพิวเตอร์กับทีมกอบกู้วิศวกรระบบ

9.2.3 ทีมกอบกู้ส่วนฐานข้อมูล (Database Team)

- ประสานงานให้ผู้ที่รับผิดชอบจัดเตรียมระบบและ Backup และ Media อื่น ๆ เช่น Harddisk ,DVD ,CD-ROM ให้พร้อมสำหรับการกอบกู้ระบบ

- ติดต่อและประสานงานไปยังหน่วยงานที่เกี่ยวข้องเพื่อขอการสนับสนุนและให้ คำปรึกษา

- รับผิดชอบในการกอบกู้ระบบงานฐานข้อมูล

9.2.4 ทีมกอบกู้ส่วนระบบเครือข่าย (Network Team)

- รับผิดชอบดูแล ตรวจสอบการทำงานของระบบเครือข่าย

- จัดเตรียมระบบเครือข่ายสื่อสารให้พร้อมสำหรับการเปิดใช้งาน

- ติดต่อและประสานงานไปยังหน่วยงานที่เกี่ยวข้องเพื่อขอการสนับสนุนและให้ คำปรึกษา

9.3 ข้อมูลการติดต่อทีมงาน (Contact Point) ทีมงานคณะผู้บริหารในสถานการณ์ฉุกเฉินหรือภัยพิบัติ (Crisis Management Team) ตามแผน BCP

9.4 การติดต่อประสานงาน (Crisis Team Communication)

<u>ภายในบริษัท</u>

การติดต่อประสานงานในแต่ละเรื่อง ก็จะใช้ทีมผู้รับผิดชอบตามโครงสร้างทีมงานกอบกู้เป็นหลัก

ภายนอกบริษัท

การติดต่อประสานกับสื่อมวลชนภายนอกองค์กรในสถานการณ์วิกฤตหรือภาวะฉุกเฉิน จะต้องไม่มีการสื่อสาร ประชาสัมพันธ์ หรือให้ข่าวกับบุคคลทั่วไปภายนอก หรือกับสื่อมวลชนต่างๆ หากมีการร้องขอข้อมูลจาก สาธารณชน หรือการร้องขอข้อมูลเพื่อจัดทำข่าวจากสื่อมวลชน

10.การจัดเตรียมอุปกรณ์ที่จำเป็น

ในการเตรียมพร้อมรับภัยพิบัติที่จะเกิดขึ้นต่อระบบเทคโนโลยีสารสนเทศฝ่ายเทคโนโลยี ซึ่งเป็นหน่วยงานหลักที่ดูแลด้านระบบคอมพิวเตอร์และระบบเครือข่ายของบริษัท ได้มีการจัดเตรียมอุปกรณ์ และเครื่องมือที่จำเป็นในกรณีคอมพิวเตอร์เกิดขัดข้องใช้งานไม่ได้ โดยมี การเตรียมอุปกรณ์ ดังนี้

- เครื่องมือและอุปกรณ์สำหรับติดตั้งระบบปฏิบัติการ/ระบบเครือข่าย/แผ่นติดตั้งระบบงานที่สำคัญ
- สื่อสำรองข้อมูลทุกระบบและระบบงานที่สำคัญ
- แผ่นโปรแกรม Antivirus/Spyware
- แผ่น Driver อุปกรณ์ต่างๆ
- ระบบสำรองไฟฉุกเฉิน (Emergency Light)
- Internal & External Harddisk สำรอง
- แผ่น Boot disk
- สำเนารายละเอียดข้อมูลการบันทึกค่าต่างๆ ในการติดตั้งอุปกรณ์ที่จำเป็น
- เอกสารคู่มืออุปกรณ์คอมพิวเตอร์แม่ข่าย และอุปกรณ์เครือข่าย
- อุปกรณ์อำนวยความสะดวกอื่น เช่น ไฟฉาย แบตเตอร์รี่เมนบอร์ด Safety Cap ถุงมือกันความร้อน ถุงมือป้องกันไฟฟ้าดูด ถังดับเพลิงเฉพาะจุด เป็นต้น

11.การปรับปรุงแผนงาน (Maintenance Guideline)

11.1 วัตถุประสงค์ของการปรับปรุงแผนการกอบกู้ข้อมูลสารสนเทศ การปรับปรุงแผนการกอบกู้ข้อมูลสารสนเทศ (Disaster Recovery Plan: DRP) ควรจะต้องทำการ ปรับปรุงอย่างสม่ำเสมอ เพื่อให้ข้อมูลความถูกต้องและสามารถใช้งานได้จริง (มากที่สุด) ซึ่งการทดสอบจะเป็นการ ตรวจสอบกระบวนการการกอบกู้ และความรู้ของผู้เข้าร่วมทดสอบในการปฏิบัติงานตามแผนฯ โดยผลลัพธ์จะบอก ถึงลำดับความสำคัญของการกอบกู้ระบบงานต่างๆ และจำเป็นจะต้องสอดคล้องกับการดำเนินงานของบริษัทฯ ในปัจจุบัน

11.2 แนวทางการปรับปรุงแผนงาน จำเป็นที่จะต้องทบทวนแผนงานทุกๆ 1 ปี ยกเว้น กรณีที่มีการเปลี่ยนแปลงที่มีนัยสำคัญจะต้อง ทบทวนใหม่ทันที ซึ่งประเด็นการพิจารณาสำหรับการปรับปรุงแผนงานนั้น มี 2 ลักษณะ ดังนี้

1) การพิจารณาปรับปรุงแผนตามกำหนดระยะเวลา

– การกำหนดช่วงเวลา จะช่วยให้สามารถวางแผนงานล่วงหน้าได้ ซึ่งควรจะกำหนดให้มีการพิจารณาปรับปรุงแผนฯ ทุก ๆ 1 ปี

- การพิจารณาแผนฯ จะช่วยให้ทราบว่าแผนงานนั้นๆ จำเป็นต้องมีการเปลี่ยนแปลงหรือไม่

- การตรวจสอบจะเน้นไปยังเหตุการณ์ที่เคยเกิดขึ้นในการพิจารณาครั้งก่อนว่าได้มีการแก้ไขปรับปรุงถูกต้องครบถ้วนหรือไม่ และต้องมีการกำหนดผู้รับผิดชอบในการแก้ไขข้อมูลดังกล่าวด้วย

2) การพิจารณาปรับปรุงแผนเร่งด่วนในกรณีที่ไม่ตรงตามกำหนดระยะเวลา

- มีการเปลี่ยนแปลงของระบบเทคโนโลยีสารสนเทศ หรือระบบโปรแกรมประยุกต์ที่เกี่ยวข้อง

- มีการเปลี่ยนแปลงผังโครงสร้างของระบบ (Configuration)

- มีการเปลี่ยนแปลงระบบเครือข่าย (Network)

- มีการเปลี่ยนแปลง โอนย้าย เลื่อนตำแหน่งหรือการลาออกของบุคลากรที่มีความเกี่ยวข้องในแผนงาน

- การเปลี่ยนแปลงหรือการปรับเปลี่ยนส่วนสำคัญของกระบวนงาน

- มีการพัฒนาหรือจัดซื้อระบบเทคโนโลยีสารสนเทศใหม่มาใช้ และยกเลิก ระบบเก่า

11.3 การวางแผนเพื่อปรับปรุงแผนงาน

- ได้มีการจัดวางแผนปรับปรุงตามแผน BCP ที่กำหนดไว้ ตามลำดับ

12.เอกสารประกอบที่ใช้ในการดำเนินการ

1. เอกสารรายการสำรองข้อมูล Backup

2. เอกสารการจัดหาระบบสนับสนุนการดำเนินการตามแผนป้องกันภัยพิบัติ (BCP)

3. ระเบียบรักษาความปลอดภัย BCP

4. เอกสารรายชื่อผู้ใช้งานระบบงาน

5. เอกสารหรือ DVD คู่มืออุปกรณ์ Hardware & Software

6. เอกสารประกอบอื่นที่เกี่ยวข้อง (ถ้ามี)

13.ผลการดำเนินการจากการกอบกู้ตามแผน DRP

แผนกู้คืนระบบเทคโนโลยีสารสนเทศเป็นแผนปฏิบัติการเพื่อลดความเสี่ยงและลดความ เสียหายทางธุรกิจให้กับองค์กรหากต้องประสบภัยพิบัติ ภายใต้การออกแบบที เป็นตาม มาตรฐาน COBIT จากการประเมินความเสี่ยงของบริษัทหากต้องเกิดความเสียหายเซิร์ฟเวอร์และประสบภัย พิบัติ ซึ่งส่งผลให้เกิดความเสียหายต่อองค์กร แผนกู้คืนระบบเทคโนโลยีสารสนเทศจึงเข้ามาเป็น เครื่องมือช่วยในการสร้างความต่อเนื่องทางธุรกิจ และมีผลการดำเนินการดังนี้

1. การสร้างแผนกู้คืนระบบเทคโนโลยีสารสนเทศ ให้กับกลุ่มบริษัทฯ ให้สำเร็จและนำมาใช้เพื่อทดสอบว่าใช้งานได้จริงตามจุดประสงค์ที่ได้กำหนดไว้ตามแบบแผน DRP

2. องค์กรมีเครื่องมือที ใช้ในการกู้คืนระบบสารสนเทศตามวัตถุประสงค์แบบแผน DRP

3. แผนกู้คืนระบบเทคโนโลยีสารสนเทศประกอบด้วยวิธีการและขั้นตอนปฏิบัติสำหรับ การกู้คืนอย่างเป็นลำดับทำให้ธุรกิจสามารถดำเนินต่อไปได้ จึงสะดวกต่อการปฏิบัติส่งผลให้ ระยะเวลาที บริษัทจะขาดความต่อเนื่องทางธุรกิจนั้นลดลง ความเสียหายที จะเกิดกับบริษัทก็ ลดลงด้วยเช่นเดียวกันดำเนินการซักซ้อมแผนกู้คืนตามแผนที่กำหนดไว้