บริษัท สแกน อินเตอร์ จำกัด (มหาชน)

แผนรับมือสถานการณ์ฉุกเฉินจากภัยพิบัติของระบบเทคโนโลยีสารสนเทศ (IT Contingency Plan)

รหัสเอกสาร : IT-02-WI วันที่บังคับใช้ : วันที่ 15 มีนาคม พ.ศ.2566 แก้ไขครั้งที่ : 00

ผู้จัดทำ	ผู้ทบทวน	ผู้อนุมัติ
นายธนศักดิ์ ฉัตรเฉลิมกิจ	นางพิมพ์วนิฎา จรัสปรีดา	ดร.ฤทธี กิจพิพิธ
ผู้จัดการแผนกเทคโนโลยีสารสนเทศ	รองประธานอาวุโส สายงานการเงินและบัญชี	ประธานเจ้าหน้าที่บริหาร
วันที่จัดทำ	วันที่ทบทวน	วันที่อนุมัติ .....

บันทึกการควบคุมการเปลี่ยนแปลงเอกสาร

แก้ไขครั้งที่	วันที่บังคับใช้	รายละเอียดการแก้ไข
00	.....	จัดทำครั้งแรก

แผนรับมือสถานการณ์ฉุกเฉินจากภัยพิบัติของระบบเทคโนโลยีสารสนเทศ
(IT Contingency Plan)

ข้อมูลสารสนเทศและระบบเทคโนโลยีสารสนเทศ ถือเป็นสิ่งที่มีความสำคัญต่อการดำเนินงานตามภารกิจของบริษัทฯ จำเป็นต้องได้รับการดูแลรักษาเพื่อให้เกิดความมั่นคงปลอดภัย สามารถนำไปใช้ประโยชน์ต่อการปฏิบัติงานได้อย่างมีประสิทธิภาพ ทางบริษัทฯ ตระหนักถึงความสำคัญของระบบเทคโนโลยีสารสนเทศ ซึ่งอาจมีปัจจัยจากภายนอกและปัจจัยภายในมากระทบทำให้ระบบเทคโนโลยีสารสนเทศ รวมทั้งระบบอุปกรณ์เครือข่ายได้รับความเสียหายได้ ดังนั้น จึงได้จัดทำแผนรับมือสถานการณ์ฉุกเฉินจากภัยพิบัติระบบเทคโนโลยีสารสนเทศ (IT Contingency Plan) เพื่อเตรียมความพร้อม และสร้างความรู้ความเข้าใจ ตลอดจนเป็นแนวทางในการดูแลรักษาระบบเทคโนโลยีสารสนเทศ ทั้งนี้ เพื่อให้ระบบเทคโนโลยีสารสนเทศสามารถดำเนินการได้อย่างต่อเนื่อง และมีประสิทธิภาพ สามารถแก้ไขสถานการณ์ได้อย่างทันท่วงที ลดความเสี่ยงที่อาจเกิดขึ้นต่อระบบเทคโนโลยีสารสนเทศของกรมส่งเสริมคุณภาพสิ่งแวดล้อม

วัตถุประสงค์

1. เพื่อเตรียมความพร้อมรับมือสถานการณ์ฉุกเฉินที่อาจจะเกิดขึ้นกับระบบเทคโนโลยีสารสนเทศขององค์กร
2. เพื่อสร้างความเข้าใจร่วมกันระหว่างผู้บริหารและผู้ปฏิบัติ ในการดูแลรักษาระบบความปลอดภัยของระบบเทคโนโลยีสารสนเทศขององค์กร
3. เพื่อใช้เป็นแนวทางในการดูแลรักษาระบบความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศขององค์กรให้มีเสถียรภาพและมีความพร้อมสาหรับการใช้งาน

ขอบเขตการดำเนินงาน

แผนรับมือสถานการณ์ฉุกเฉินจากภัยพิบัติ ระบบเทคโนโลยีสารสนเทศ (IT Contingency Plan) ที่บริษัทฯจัดทำขึ้นสำหรับเป็นกรอบแนวทางในการดูแลรักษาและแก้ไขปัญหาที่อาจจะส่งผลกระทบต่อระบบเทคโนโลยีสารสนเทศของกรมฯ ประกอบด้วย

1. การวิเคราะห์และประเมินความรุนแรงของเหตุการณ์ภัยพิบัติ
2. ขั้นตอนและแนวทางการป้องกันเบื้องต้น
3. การเตรียมความพร้อม
4. การติดตามและรายงานผล

บันทึกการควบคุมการเปลี่ยนแปลงเอกสาร

แก้ไขครั้งที่	วันที่บังคับใช้	รายละเอียดการแก้ไข
00	.....	จัดทำครั้งแรก

แผนรับมือสถานการณ์ฉุกเฉินจากภัยพิบัติของระบบเทคโนโลยีสารสนเทศ
(IT Contingency Plan)

ข้อมูลสารสนเทศและระบบเทคโนโลยีสารสนเทศ ถือเป็นสิ่งที่มีความสำคัญต่อการดำเนินงานตามภารกิจของบริษัทฯ จำเป็นต้องได้รับการดูแลรักษาเพื่อให้เกิดความมั่นคงปลอดภัย สามารถนำไปใช้ประโยชน์ต่อการปฏิบัติงานได้อย่างมีประสิทธิภาพ ทางบริษัทฯ ตระหนักถึงความสำคัญของระบบเทคโนโลยีสารสนเทศ ซึ่งอาจมีปัจจัยจากภายนอกและปัจจัยภายในมากระทบทำให้ระบบเทคโนโลยีสารสนเทศ รวมทั้งระบบอุปกรณ์เครือข่ายได้รับความเสียหายได้ ดังนั้น จึงได้จัดทำแผนรับมือสถานการณ์ฉุกเฉินจากภัยพิบัติระบบเทคโนโลยีสารสนเทศ (IT Contingency Plan) เพื่อเตรียมความพร้อม และสร้างความรู้ความเข้าใจ ตลอดจนเป็นแนวทางในการดูแลรักษาระบบเทคโนโลยีสารสนเทศ ทั้งนี้ เพื่อให้ระบบเทคโนโลยีสารสนเทศสามารถดำเนินการได้อย่างต่อเนื่อง และมีประสิทธิภาพ สามารถแก้ไขสถานการณ์ได้อย่างทันท่วงที ลดความเสี่ยงที่อาจเกิดขึ้นต่อระบบเทคโนโลยีสารสนเทศของกรมส่งเสริมคุณภาพสิ่งแวดล้อม

วัตถุประสงค์

1. เพื่อเตรียมความพร้อมรับมือสถานการณ์ฉุกเฉินที่อาจจะเกิดขึ้นกับระบบเทคโนโลยีสารสนเทศขององค์กร
2. เพื่อสร้างความเข้าใจร่วมกันระหว่างผู้บริหารและผู้ปฏิบัติ ในการดูแลรักษาระบบความปลอดภัยของระบบเทคโนโลยีสารสนเทศขององค์กร
3. เพื่อใช้เป็นแนวทางในการดูแลรักษาระบบความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศขององค์กรให้มีเสถียรภาพและมีความพร้อมสาหรับการใช้งาน

ขอบเขตการดำเนินงาน

แผนรับมือสถานการณ์ฉุกเฉินจากภัยพิบัติ ระบบเทคโนโลยีสารสนเทศ (IT Contingency Plan) ที่บริษัทฯจัดทำขึ้นสำหรับเป็นกรอบแนวทางในการดูแลรักษาและแก้ไขปัญหาที่อาจจะส่งผลกระทบต่อระบบเทคโนโลยีสารสนเทศของกรมฯ ประกอบด้วย

1. การวิเคราะห์และประเมินความรุนแรงของเหตุการณ์ภัยพิบัติ
2. ขั้นตอนและแนวทางการป้องกันเบื้องต้น
3. การเตรียมความพร้อม
4. การติดตามและรายงานผล

1. การวิเคราะห์ปัญหาความรุนแรงของเหตุการณ์ภัยพิบัติ

1.1 วิเคราะห์เหตุการณ์ภัยพิบัติ ภัยพิบัติที่อาจก่อให้เกิดความเสียหายกับระบบเทคโนโลยีสารสนเทศของบริษัทฯ จำแนกเป็น 2 กลุ่มหลักๆ ได้แก่

ภัยพิบัติจากภายนอก

1) ภัยธรรมชาติและการเกิดสถานการณ์ความไม่สงบที่กระทบต่อสถานที่ตั้งของเครื่องแม่ข่าย ได้แก่ ภัยพิบัติ อัคคีภัย อุทกภัย การจลาจล ชุมนุมประท้วง แผ่นดินไหว ฯลฯ

2) ระบบเครื่องแม่ข่ายที่เชื่อมต่อระบบอินเตอร์เน็ตเกิดความขัดข้อง

3) การบุกรุกหรือโจมตีระบบควบคุมเทคโนโลยีสารสนเทศจากภายนอก เพื่อสร้างความเสียหายหรือทำลายระบบข้อมูล

4) ระบบกระแสไฟฟ้าขัดข้อง / ไฟฟ้าดับ / ไฟกระชาก

5) ไวรัสคอมพิวเตอร์

ภัยพิบัติจากภายใน

1) ระบบเครื่องแม่ข่ายหลัก ระบบฐานข้อมูลหลักเสียหาย ถูกทำลาย

2) ไวรัสคอมพิวเตอร์จากผู้ใช้งานภายในบริษัทฯ

3) เจ้าหน้าที่หรือบุคลากรของบริษัทฯ ขาดความรู้ความเข้าใจในการใช้อุปกรณ์คอมพิวเตอร์ ทั้งด้านฮาร์ดแวร์และซอฟต์แวร์ อาจทำให้ระบบเทคโนโลยีสารสนเทศเสียหาย

2. ขั้นตอนและแนวทางการป้องกันเบื้องต้น

2.1 การประกาศใช้แผน

องค์กร มีการประกาศใช้แผนรับสถานการณ์ฉุกเฉินจากภัยพิบัติระบบเทคโนโลยีสารสนเทศอย่างเป็นทางการ เพื่อให้เจ้าหน้าที่ทุกคนทราบและปฏิบัติตามอย่างเคร่งครัด โดยเมื่อเกิดเหตุการณ์ฉุกเฉิน ผู้จัดการฝ่ายเทคโนโลยีสารสนจะทำการแจ้งให้ผู้บริหารเทคโนโลยีสารสนเทศระดับสูงของบริษัทฯ ทราบ เพื่อพิจารณาประกาศใช้แผนต่อไป

2.2 กำหนดขั้นตอนการดำเนินงาน

ฝ่ายเทคโนโลยีสารสนเทศจัดเตรียมขั้นตอนการปฏิบัติเมื่อเกิดเหตุการณ์ฉุกเฉินหรือผิดปกติในบริษัทฯ โดยกาหนดขั้นตอนการปฏิบัติที่เหมาะสมต่อสถานการณ์ต่างๆ ที่เกิดขึ้น รวบรวมเหตุการณ์ การระบุที่มาของผู้บุกรุก เพื่อให้สามารถยุติเหตุการณ์ที่เกิดขึ้นได้อย่างทันเวลา รวมถึงการเตรียมอุปกรณ์สำรองเพื่อใช้ในการกู้คืนระบบ

2.3 การติดต่อประสานงาน

มีการจัดทำข้อมูลรายชื่อหน่วยงานภายนอก เพื่อใช้สาหรับการติดต่อทางด้านความมั่นคงปลอดภัย กรณีที่มีความจำเป็นฉุกเฉิน เช่น การไฟฟ้า สถานีดับเพลิง สถานีตารวจ เป็นต้น

2.4 การจัดเตรียมอุปกรณ์

ฝ่ายเทคโนโลยีสารสนเทศ ซึ่งเป็นหน่วยงานหลักที่ดูแลระบบเทคโนโลยีสารสนเทศ ระบบเครือข่าย คอมพิวเตอร์ ได้มีการจัดเตรียมอุปกรณ์และเครื่องมือที่จำเป็นในกรณีคอมพิวเตอร์หรืออุปกรณ์เครือข่ายเกิดขัดข้องใช้งานไม่ได้ ดังนี้

- เครื่องคอมพิวเตอร์ PC / เครื่องคอมพิวเตอร์ Notebook
- แผ่นติดตั้งระบบปฏิบัติการ / ระบบปฏิบัติการของเครือข่าย / แผ่นติดตั้งระบบงานที่สำคัญ
- อุปกรณ์สำรองข้อมูลและระบบงานที่สำคัญ
- โปรแกรม antivirus
- Driver อุปกรณ์ต่างๆ
- ระบบสำรองไฟฟ้าอัตโนมัติ
- อุปกรณ์สำรองต่างๆ ของเครื่องคอมพิวเตอร์

2.5 การสำรองข้อมูล

เพื่อป้องกันความเสียหายที่อาจเกิดขึ้นเมื่อข้อมูลเกิดความเสียหาย ถูกทำลายจากไวรัส ถูกแทรกแซงจากผู้บุกรุกทำลายข้อมูล หรือได้รับความเสียหายจากภัยพิบัติ โดยสามารถนำข้อมูลที่มีปัญหากลับมาใช้งานได้ โดยบริษัทฯ มีนโยบายการสำรองข้อมูลระบบคอมพิวเตอร์ และแผนการสำรองข้อมูล ดังนี้

1) การสำรองข้อมูล (Backup) เต็มรูปแบบทุกวัน ในทุก Server ที่ให้บริการ ดังนี้
   - มีการสำรองข้อมูลชุดที่ 1 ที่ห้องควบคุมระบบเครือข่ายส่วนกลางในรูปแบบ Virtual Server (VMWare) บน Hardware ในตัวเอง ซึ่งสามารถ Restore ข้อมูลย้อนหลังไม่น้อยกว่า 30 วัน
   - มีการสำรองข้อมูลชุดที่ 2 ที่ห้องควบคุมระบบเครือข่ายส่วนกลางในรูปแบบ Replicate Server (VMWare) ไปยัง Hardware อีกตัว ซึ่งสามารถ Restore ข้อมูลย้อนหลังไม่น้อยกว่า 7 วัน
   - มีการสำรองข้อมูลชุดที่ 3 ไปยังไซค์สำรองข้อมูลระยะไกล (โทรน้อย) ในรูปแบบ Replicate Server (VMWare) ซึ่งสามารถ Restore ข้อมูลย้อนหลังไม่น้อยกว่า 7 วัน
2) การสำรองข้อมูลค่าการตั้งค่า Configuration ของตัวอุปกรณ์
   - มีการสำรองค่า Configuration อุปกรณ์ Network ในทุกๆ เดือน
   - มีการสำรองค่า Configuration อุปกรณ์ Server ในทุกๆ เดือน

2.6 การป้องกันและกำจัดไวรัส

มีการติดตั้งซอฟต์แวร์ป้องกันและกำจัดไวรัส สำหรับเครื่องคอมพิวเตอร์แม่ข่ายและเครื่องคอมพิวเตอร์ลูกข่ายที่เชื่อมต่อในระบบเครือข่าย โดยผู้ใช้งานต้องระมัดระวังในการใช้งานระบบคอมพิวเตอร์ โดยเฉพาะในการเชื่อมต่ออินเตอร์เน็ต และเพื่อไม่ให้เป็นช่องทางให้ผู้บุกรุกสามารถเข้ามาทำลายระบบได้

2.7 การป้องกันการบุกรุก และภัยคุกคามทางคอมพิวเตอร์

เพื่อเป็นการสร้างความปลอดภัยให้กับระบบเทคโนโลยีสารสนเทศและระบบเครือข่าย มีแนวทางดังนี้

1) กาหนดมาตรการควบคุมการเข้า – ออก ห้องควบคุมระบบเครือข่ายและการป้องกันความเสียหาย โดยห้องควบคุมจะมีกุญแจ และ Keycard ส่วนกลางเพียง 1 ชุดเท่านั้น กรณีที่ผู้เกี่ยวข้องต้องการเข้าไปในห้องควบคุม ต้องลงชื่อเบิกกุญแจ และ Keycard ในสมุดควบคุมการเข้า – ออก ห้ามบุคคลที่ไม่มีอานาจหน้าที่เกี่ยวข้องเข้าไปในห้องควบคุมระบบเครือข่าย หากจำเป็นให้เจ้าหน้าที่ของฝ่ายเทคโนโลยีสารสนเทศ เป็นผู้รับผิดชอบพาเข้าไป และในห้องควบคุมมีการติดตั้งกล้องโทรทัศน์วงจรปิด

2) มีการติดตั้งอุปกรณ์ป้องกันการบุกรุก (Firewall) เพื่อป้องกันไม่ให้ผู้ที่ไม่ได้รับอนุญาตจากระบบเครือข่ายอินเตอร์เน็ต สามารถเข้าสู่ระบบสารสนเทศและระบบเครือข่ายคอมพิวเตอร์ได้ โดยกาหนดให้ Firewall ควบคุมการเข้า-ออก หรือการควบคุมการรับ-ส่งข้อมูล ในระบบเครือข่าย และเปิดใช้งานตลอดเวลา

3) มีเจ้าหน้าที่ดูแลระบบเครือข่าย ทำการตรวจสอบการใช้งานข้อมูลบนเครือข่ายอินเตอร์เน็ตของบริษัทฯ เพื่อตรวจสอบการใช้งานบนเครือข่ายว่ามีปริมาณมากผิดปกติ หรือการเรียกใช้ระบบสารสนเทศมีความถี่ในการเรียกใช้ผิดปกติ เพื่อจะได้สรุปหาสาเหตุและหาวิธีการป้องกันต่อไป

2.8 การป้องกันและแก้ไขปัญหาที่เกิดจากกระแสไฟฟ้าขัดข้อง

เพื่อเป็นการป้องกันและแก้ไขปัญหาจากกระแสไฟฟ้าซึ่งอาจสร้างความเสียหายแก่ระบบเทคโนโลยีสารสนเทศและอุปกรณ์เครือข่ายคอมพิวเตอร์ ได้กำหนดแนวทาง ดังนี้

1) ติดตั้งเครื่องสำรองไฟฟ้าอัตโนมัติ เพื่อป้องกันความเสียหายที่อาจเกิดขึ้นกับอุปกรณ์คอมพิวเตอร์ อุปกรณ์เครือข่าย หรือการประมวลผลของระบบคอมพิวเตอร์ ในส่วนของเครื่องคอมพิวเตอร์แม่ข่าย (Server) ซึ่งมีระยะเวลาการสำรองไฟฟ้าได้ประมาณ 120 นาที

2) ติดตั้งเครื่องกำเนิดไฟฟ้าสำรอง (Generator)

3) เปิดเครื่องสำรองไฟฟ้า (UPS) ตลอดระยะเวลาในการใช้งานเครื่องคอมพิวเตอร์ และบำรุงรักษาเครื่องสำรองไฟฟ้าให้อยู่ในสภาพพร้อมใช้งานอยู่เสมอ

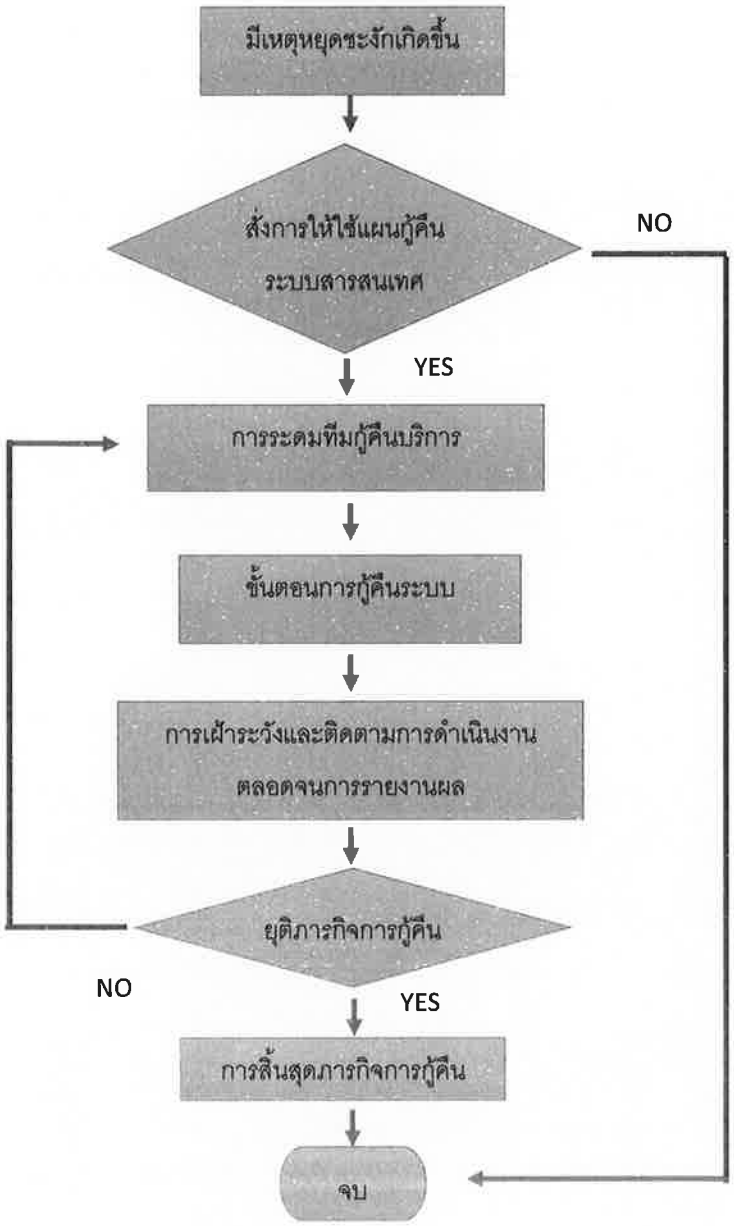
4) เมื่อเกิดกระแสไฟฟ้าดับ ให้ผู้ใช้รีบบันทึกข้อมูลทันที และปิดเครื่องคอมพิวเตอร์และอุปกรณ์ต่างๆ

3. การติดตามและรายงานผล

กำหนดให้เจ้าหน้าที่ทีมผู้รับผิดชอบรายงานผลการดาเนินการหรือการตรวจสอบเมื่อเกิดเหตุการณ์หรือภัยพิบัติฉุกเฉิน ให้ผู้จัดการฝ่ายเทคโนโลยีสารสนเทศเพื่อนำเสนอรายงานสรุปให้ผู้บริหารระดับสูงทราบ เพื่อที่จะนามาปรับปรุงพัฒนาแผนรักษาความปลอดภัยระบบเทคโนโลยีสารสนเทศให้มีประสิทธิภาพ สามารถนำมาใช้งานได้ทันที ในกรณีที่เกิดภัยพิบัติในครั้งต่อไป

4. ขั้นตอนการปฏิบัติเมื่อเกิดเหตุการณ์ฉุกเฉิน

เมื่อมีคำสั่งให้ใช้แผนกู้คืนระบบสารสนเทศฉบับนี้แล้ว รูปด้านล่างแสดงขั้นตอนการดำเนินการต่างๆ เพื่อนำบริการระบบสารสนเทศที่เกิดการหยุดชะงักไป กลับคืนมาให้บริการได้อีกครั้งหนึ่ง



เครื่องเซิร์ฟเวอร์และระบบบริการที่ต้องดำเนินการกู้คืนระบบให้เสร็จภายในระยะเวลาที่กำหนดตามตารางด้านล่าง

ID	ชื่อเซิร์ฟเวอร์ / ชื่อระบบ	ระยะเวลาการกู้คืน	เป้าหมายขั้นต่ำในการดำเนินธุรกิจอย่างต่อเนื่อง	ระยะเวลาสูงสุดที่ยอมให้ข้อมูลเสียหาย
1	AD01 (Active Directory Service)	4 ชม.	ระบบงานมีขีดความสามารถที่ร้อยละ 70 เมื่อเทียบกับระบบหลัก	14 วัน
2	ERPAX (Microsoft Dynamics AX)	12 ชม.	ระบบงานมีขีดความสามารถที่ร้อยละ 70 เมื่อเทียบกับระบบหลัก	7 วัน
3	ERPDB (SQL Database Server)	12 ชม.	ระบบงานมีขีดความสามารถที่ร้อยละ 70 เมื่อเทียบกับระบบหลัก	7 วัน
4	Payroll (ระบบเงินเดือน)	12 ชม.	ระบบงานมีขีดความสามารถที่ร้อยละ 70 เมื่อเทียบกับระบบหลัก	14 วัน

ทีมกู้คืนระบบบริการ บทบาท และหน้าที่ความรับผิดชอบ ประกอบด้วยบุคคลากรตามที่ปรากฏในตารางนี้

ลำดับที่	ชื่อ	บทบาท และหน้าที่ความรับผิดชอบ
1.	หัวหน้าทีมกู้คืนระบบ ผู้จัดฝ่ายเทคโนโลยีสารสนเทศ (นายธนศักดิ์ ฉัตรเฉลิมกิจ)	○ ประเมินสถานการณ์ที่เกิดขึ้นว่ามีผลกระทบและความรุนแรงในระดับใด ○ ระดับลูกทีมทั้งหมดเพื่อลงพื้นที่ปฏิบัติการประสานงานและสั่งการให้ลูกทีมร่วมกันดำเนินการแก้ไขปัญหาที่พบ ○ รายงานสถานการณ์การกู้คืนระบบให้หน่วยติดตามสถานการณ์ ประธานคณะทำงานและคณะทำงานได้รับทราบเป็นระยะ ๆ

		○ ประสานงานกับฝ่ายอาคารสถานที่ และฝ่าย รปภ. เพื่อขอให้ช่วยดำเนินการในเรื่องต่างๆ อาทิ ตรวจสอบระบบไฟฟ้า ระบบโทรศัพย์ ระบบปรับอากาศ การรักษาความปลอดภัย หรืออื่นๆ ที่เกี่ยวข้อง ○ สั่งการให้ลูกทีมตรวจสอบและเตรียมความพร้อมของระบบเทคโนโลยีสารสนเทศต่าง ๆ ในห้องคอบคุมระบบเครื่อข่ายสำรอง ○ จัดทำรายงาน After Action Report ภายหลังสถานการณ์สิ้นสุดลง
2.	ทีมติดตั้งเซิร์ฟเวอร์ เครือข่าย และแอพพลิเคชั่นฐานข้อมูล เจ้าหน้าที่สนับสนุน 1. นายธนศักดิ์ ฉัตรเฉลิมกิจ 2. นายธวัชชัย ชัยช่อฟ้า 3. กันต์กวี กล่ำเพ็ชร์	○ สำรวจและประเมินความเสียหายของฮาร์แวร์ อุปกรณ์ข้อมูล และ/หรือซอฟต์แวร์ต่าง ๆ ของระบบที่กิดความเสียหาย และจำเป็นต้องแก้ไขหรือติดตั้งกลับคืน ○ กำหนดรายการของฮาร์ดแวร์ อุปกรณ์ ข้อมูล และ/หรือซอฟต์แวร์ต่าง ๆ ที่จำเป็นต้องใช้ในการกู้คืน ○ แจ้งรายการอาร์ตแวร์หรืออุปกรณ์ที่ต้องการพร้อมทั้งคุณลักษณะให้ทีมการจัดการทั่วไปช่วยดำเนินการจัดหาให้ ○ ติดตั้งฮาร์แวร์ อุปกรณ์ และ/หรือซอฟต์แวร์ที่เกี่ยวข้องกับระบบ โดยติดตั้งให้เหมือนเดิมหรือใกล้เคียงกับระบบเดิมมากที่สุด ○ นำข้อมูลล่าสุดที่สำรองเก็บไว้มาทำการติดตั้งกลับคืนตามความจำเป็น

- ทีมติดตั้งเซิร์ฟเวอร์ และเครือข่าย มีหน้าที่ดังนี้

1. สำรวจ และประเมินความเสียหายของฮาร์ดแวร์ อุปกรณ์ ข้อมูล และ/หรือ ซอฟต์แวร์ ต่าง ๆ ของระบบที่เกิดความเสียหาย และจำเป็นต้องแก้ไข หรือติดตั้งกลับคืน

2. กำหนดรายการของฮาร์ดแวร์ อุปกรณ์ ข้อมูล และ/หรือ ซอฟต์แวร์ต่าง ๆ ที่จำเป็นต้องใช้ในการกู้คืน

3. แจ้งรายการฮาร์ดแวร์หรืออุปกรณ์ พร้อมทั้งคุณลักษณะที่ต้องการให้หัวหน้าทีมกู้คืนระบบ ช่วยดำเนินการจัดหาให้

4. ติดตั้งฮาร์ดแวร์ อุปกรณ์ และ/หรือ ซอฟต์แวร์ที่เกี่ยวข้องกับระบบ โดยติดตั้งให้ เหมือนเดิม หรือใกล้เคียงกับระบบเดิมให้มากที่สุด

- ทีมติดตั้งแอพพลิเคชันฐานข้อมูล มีหน้าที่ดังนี้

1. ติดตั้งและปรับแต่งแอพพลิเคชันให้เหมือนระบบเดิมมากที่สุด

2. ทดสอบฟังก์ชันการทำงานต่าง ๆ ของระบบ เพื่อดูว่าสามารถใช้งานได้ครบถ้วนหรือไม่

3. นำข้อมูลล่าสุด (ของฐานข้อมูล) ที่สำรองเก็บไว้มาทำการติดตั้งกลับคืนตามความจำเป็น

4. พยายามกู้คืนข้อมูลของระบบให้กลับไปสู่จุด ณ เวลาที่เกิดอุบัติการณ์ขึ้น

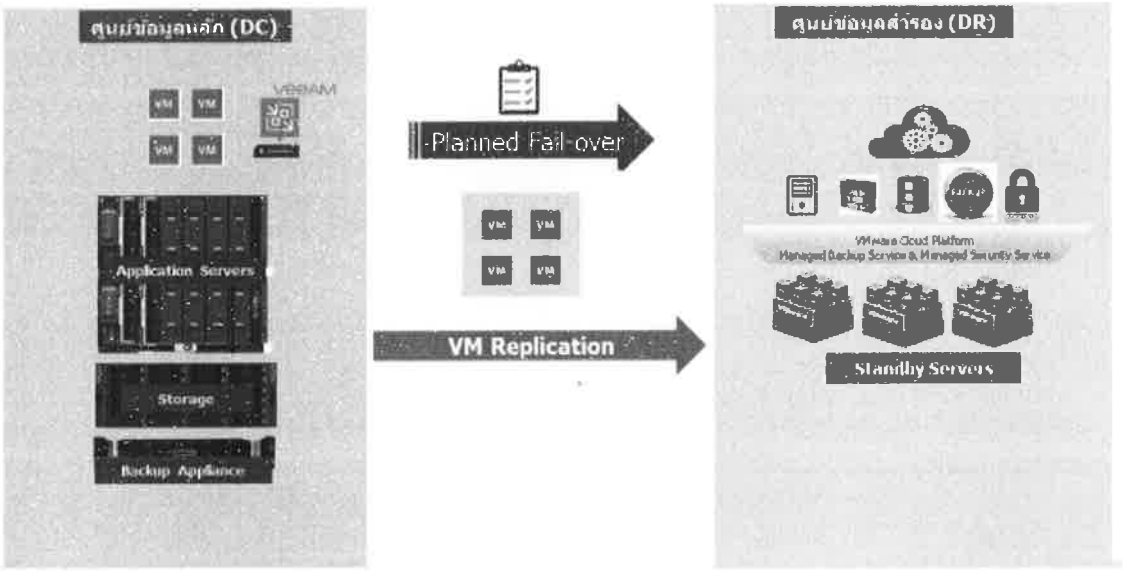
5. ตรวจสอบดูความถูกต้องของข้อมูลที่ทำการติดตั้งกลับคืน

6. ทดสอบระบบร่วมกับผู้ใช้งาน

ขั้นตอนการกู้คืนบริการระบบสารสนเทศ

ขั้นตอนนี้เป็นการกู้คืนบริการระบบสารสนเทศที่ไซต์สำรองตามที่กำหนดไว้ เพื่อให้สามารถกลับคืนมาให้บริการได้ตามระยะเวลาที่กำหนด เป้าหมายของการกู้คืนที่กำหนดไว้ในรูปฝั่งขวามือคือไซต์สำรอง (DR) ของบริการระบบสารสนเทศ ซึ่งได้มีการเตรียมการ เซิร์ฟเวอร์ และอุปกรณ์ต่าง ๆ ตามที่ปรากฏในรูป เพื่อให้สามารถกู้คืนบริการให้กลับคืนมาให้บริการได้ตามปกติ

แผนภาพแสดงการทำแผนรองรับภัยพิบัติและสถานการณ์ฉุกเฉิน (Business Continuity Plan)



การเฝ้าระวัง ติดตามการดำเนินงาน และการรายงานผล

เมื่อแผนกู้คืนบริการได้เริ่มต้นดำเนินการแล้ว หัวหน้าทีมกู้คืนระบบ จำเป็นต้องมีการเฝ้าระวังและติดตามการดำเนินงานต่าง ๆ ของลูกทีม แจ้งความคืบหน้าให้หน่วยติดตามสถานการณ์รับทราบเพื่อรายงานต่อคณะกรรมการบริหารสถานการณ์ฉุกเฉินต่อไป ตลอดจนสื่อสารไปยังผู้ที่เกียวข้องในทุกระดับตามความจำเป็น

การสิ้นสุดภารกิจการกู้คืนบริการ

ภายหลังจากที่เสร็จสิ้นการกู้คืนบริการแล้วทีมกู้คืนบริการจะแจ้งให้หน่วยติดตามสถานการณ์ เพื่อรายงานต่อคณะกรรมการบริหารสถานการณ์ฉุกเฉินให้ได้รับทราบต่อไป คณะกรรมการบริหารต้องมีมติยุติการรับมือกับอุบัติการณ์ และสิ้นสุดปฏิบัติการ

ข้อมูลในตารางด้านล่างนี้เป็นข้อมูลการติดต่อคณะกรรมการบริหารสถานการณ์ฉุกเฉิน

ชื่อ / ตำแหน่ง	บทบาทหน้าที่	เบอร์โทรศัพย์	E-Mail
นางพิมพ์วนิฎา จรัสปรีดา (รองประธานอาวุโส สายงานการเงินและบัญชี)	กรรมการบริหารสถานการณ์ฉุกเฉิน	0614044745	pimwanitar@scan-inter.com
นางสาวกาญจนา คงชัยทรัพย์ (รองประธานสายงานทรัพยากรมนุษย์)	กรรมการบริหารสถานการณ์ฉุกเฉิน	0655246136	kanchana.k@scan-inter.com

ตารางด้านล่างนี้เป็นข้อมูลการติดต่อสมาชิกทีมกู้คืนบริการระบบสารสนเทศ

ชื่อ	บทบาทหน้าที่ในแผน	เบอร์โทรศัพย์	E-Mail
นายธนศักดิ์ ฉัตรเฉลิมกิจ	หัวหน้าทีมกู้คืนระบบ	0824883309	thanasak@scan-inter.com
นายธวัชชัย ชัยช่อฟ้า	ผู้ช่วยการกู้คืนระบบ	0855121386	tawatchai@scan-inter.com
นายกันต์กวี กล่ำเพ็ชร์	ผู้ช่วยการกู้คืนระบบ	0882809268	gunkawee.kl@scan-inter.com

จึงประกาศมาเพื่อทราบและถือปฏิบัติโดยทั่วกัน

(ดร.ฤทธี กิจพิพิธ)

ประธานเจ้าหน้าที่บริหาร