แผนแก้ไขปัญหาระบบเทคโนโลยีสารสนเทศ เมื่อเกิดเหตุการณ์ฉุกเฉิน

(IT Contingency Plan) ของบริษัท บางกอกคริสตัล จำกัด

วัตถุประสงค์

1. เพื่อสร้างความเข้าใจร่วมกันระหว่างผู้บริหารและผู้ปฏิบัติในการดูแลรักษาระบบความปลอดภัยของระบบเทคโนโลยีสารสนเทศของบริษัท บางกอกคริสตัล จำกัด
2. เพื่อลดความเสียหายที่อาจจะเกิดแก่ระบบเทคโนโลยีสารสนเทศของบริษัท บางกอกคริสตัล จำกัด
3. เพื่อให้ระบบเทคโนโลยีสารสนเทศสามารถดำเนินการได้อย่างต่อเนื่อง และสามารถตอบสนองสถานการณ์ได้อย่างทันท่วงที

กรอบแนวทางในการจัดทำแผน

การจัดทำแผนรับสถานการณ์ฉุกเฉิน ส่งผลกระทบต่อระบบเทคโนโลยีสารสนเทศและการสื่อสาร (IT Contingency Plan) มีแนวทางในการดูแลรักษาและแก้ไขปัญหาที่อาจจะส่งผลกระทบต่อฐานข้อมูลและระบบเทคโนโลยีสารสนเทศขององค์กร ดังนี้

1. การวิเคราะห์และประเมินความรุนแรงของเหตุการณ์
2. แนวทางการป้องกันและเตรียมการเบื้องต้น
3. การเตรียมความพร้อม
4. กำหนดผู้รับผิดชอบเมื่อเกิดสถานการณ์ฉุกเฉิน
5. มาตรการในการป้องกันและแก้ไขปัญหา
6. แผนกู้คืนระบบกลับสู่สภาพปกติเดิม
7. การติดตามและรายงานผล

ภัยที่ก่อให้เกิดความเสียหายกับระบบเทคโนโลยีสารสนเทศของคณะวิทยาศาสตร์ สามารถจำแนกได้ดังนี้

1. ภัยธรรมชาติที่กระทำต่ออาคารสถานที่ตั้งของเครื่อง Server ได้แก่ อัคคีภัย อุทกภัย การป้องกันความชื้นและอุณหภูมิที่ไม่เหมาะสม แมลงสัตว์กัดแทะ เป็นต้น
2. ระบบกระแสไฟฟ้าขัดข้อง / ไฟฟ้าดับ

3. การบุกรุกหรือโจมตีจากภายนอก เพื่อเข้าถึงหรือควบคุมระบบเทคโนโลยีสารสนเทศ รวมทั้งสร้างความเสียหายหรือทำลายระบบข้อมูล
4. ไวรัสคอมพิวเตอร์
5. ระบบเสียหายจากภัยสงครามเหตุจลาจลและการเกิดสถานการณ์ความไม่สงบ
6. ระบบแม่ข่ายหลัก ระบบฐานข้อมูลหลักเสียหาย หรือข้อมูลถูกทำลาย

แนวทางการป้องกันความเสียหายจากภัยพิบัติ

1. ภัยธรรมชาติที่กระทำต่ออาคารสถานที่ตั้งของเครื่อง Server ได้แก่ อัคคีภัย อุทกภัยและการป้องกันความชื้นและอุณหภูมิที่ไม่เหมาะสม เป็นต้น
   1.1 ติดตั้งเครื่องวัด ความชื่น อุณหภูมิ
   1.2 เครื่องคอมพิวเตอร์แม่ข่ายต้องไม่อยู่ในบริเวณที่น้ำท่วมถึง
   1.3 เปิดเครื่องปรับอากาศพร้อมอุปกรณ์ควบคุมความชื้น สำหรับเครื่อง Server ตลอด 24 ชั่วโมง
2. ระบบการสื่อสารของเครื่องคอมพิวเตอร์ ที่เชื่อมต่อกับระบบเครือข่าย
   2.1 การตรวจสอบระบบเครือข่ายให้สามารถใช้งานได้ตลอดเวลา
   2.2 ย้าย ระบบบริการ Software ไปยังระบบ Cloud
   2.3 จัดให้มีอุปกรณ์ของระบบเครือข่ายสำรอง สำหรับใช้ในกรณีที่อุปกรณ์หลักไม่สามารถใช้งานได้
   2.4 ประสานงานกับหน่วยงานที่เกี่ยวข้องเพื่อแก้ไขปัญหา
3. ระบบกระแสไฟฟ้าขัดข้อง / ไฟฟ้าดับ
   3.1 ติดตั้งเครื่องสำรองไฟฟ้า (UPS) เพื่อป้องกันความเสียหายที่อาจเกิดขึ้นกับ เครื่องคอมพิวเตอร์ (Server) ซึ่งต้องมีระยะเวลาในการสำรองไฟฟ้าได้ไม่น้อยกว่า 15 นาที
   3.2 เครื่องสำรองไฟฟ้า (UPS) มีระบบตรวจสอบเครื่องสำรองไฟ (แจ้งเตือน เปลี่ยน Battery)
4. การบุกรุกหรือโจมตีจากภายนอก เพื่อเข้าถึงหรือควบคุมระบบเทคโนโลยีสารสนเทศ รวมทั้งสร้างความเสียหายหรือทำลายระบบข้อมูล
   4.1 ออโต้อัพเดท Security patch / Antivirus เพื่อปิดกั้นช่องโหว่และจุดอ่อนของระบบปฏิบัติการ
   4.2 เปิดใช้งาน Firewall ของเครื่องแม่ข่ายตลอดเวลา เพื่อป้องกันผู้ที่มิได้รับอนุญาตจากระบบเครือข่าย

5. ระบบเสียหายจากภัยสงคราม/เหตุจลาจล และการเกิดสถานการณ์ความไม่สงบการสำรองข้อมูล มีการจัดเก็บเป็น 2 แหล่ง
    1. ภายใน Backup Server
    2. อับโหลด ขึ้น Cloud

7. ระบบแม่ข่ายหลัก ระบบฐานข้อมูลหลักเสียหาย หรือข้อมูลถูกทำลาย

การสำรองข้อมูลอัตโนมัติ โดยระบบเครื่องประมวลผลแม่ข่ายจะสำรองข้อมูลไว้ในสื่อบันทึกข้อมูลทุกวัน กำหนดระยะเวลาสำรองข้อมูล เริ่มตั้งแต่เวลา 18.00-7.00 น. หรือ ตามเหมาะสม

ขั้นตอนปฏิบัติ

1. **กรณีเครื่อง Server และอุปกรณ์เครือข่าย ภายในโรงงาน พบปัญหาที่อาจจะเกิดความเสียหาย**
    1.1 ตัดการเชื่อมต่อระบบ Server แล้วปิดอุปกรณ์เครือข่ายและเครื่อง Server ตามลำดับความสำคัญของ การให้บริการ
    1.2 ถ้าไฟฟ้าดับ/ไฟฟ้าตก ให้ปิดเครื่อง Server และอุปกรณ์เครือข่ายโดยพิจารณาตามความสำคัญของการให้บริการ ระยะเวลาที่ไฟฟ้าดับ และประสิทธิภาพของเครื่องสำรองไฟฟ้า
    1.3 ปิดระบบจ่ายไฟ ในกรณีไฟไหม้ให้ใช้น้ำยาดับเพลิงฉีดควบคุมเพลิงโดยเร็ว
    1.4 รีบขนย้ายเครื่องไปไว้ในที่ปลอดภัย
    1.5 ในกรณีอุปกรณ์ด้านฮาร์ดแวร์เสีย ให้รีบหาอุปกรณ์สำรอง นำอุปกรณ์มาเปลี่ยนโดยเร็วที่สุด
    1.6 ผู้ดูแลระบบ ต้องแจ้งให้ผู้บังคับบัญชาทราบโดยเร็ว
2. **กรณีเครื่อง Server ให้บริการภายนอก (BIS) ไม่สามารถให้บริการได้**
    2.1 ตรวจสอบว่าเป็นที่เครือข่ายภายในหรือไม่
    2.2 ให้เครื่องลูกข่ายเปลี่ยน Server เชื่อมต่อไปยัง Server สำรองใช้งาน
    2.3 ผู้ดูแลระบบให้บริการ BIS แจ้งผู้ใช้งานให้ทราบ เพื่อใช้งาน Server สำรอง
3. **กรณี Email ไม่สามารถให้บริการได้**
    3.1 ตรวจสอบว่าเป็นที่เครือข่ายภายในหรือไม่
    3.2 ติดต่อผู้ดูแล ระบบ G-Suite ของ บางกอกคริสตัล
    3.3 แจ้งให้ผู้ใช้งาน ให้ทราบปัญหา

แผนกู้คืนระบบคอมพิวเตอร์กลับสู่สภาวะปกติเดิม

1. การคืนระบบเครื่อง Server และอุปกรณ์เครือข่ายภายใน โรงงาน โดยปกติระบบเครื่อง Server และอุปกรณ์ เครือข่าย ต้องอยู่ในสภาพที่พร้อมรองรับการให้บริการกับเครื่องลูกข่ายได้ตลอดเวลา 24 ชั่วโมง หากไม่สามารถให้บริการได้ ต้องรีบกู้ระบบคืนให้ได้เร็วที่สุด เพื่อทำให้ระบบการทำงานของเครื่องคอมพิวเตอร์และข้อมูลกลับสู่สภาพเดิม
2. บริการ Server ให้บริการภายนอก (BIS)
   ติดต่อ ผู้ให้บริการ INET Internet Thailand Public Company Limited
   Email noc@inet.co.th
   Tel. (662) 257 7000
3. บริการ Email G-Suite ของ Google
   Email info@tectony.co.th
   ติดต่อ เทคโทนี่ จำกัด
   Tel. 086-416-4295, 02-4027-1000

ระบบเสียหายหรือหยุดทำงาน โดยดำเนินการ ดังนี้

1. จัดหาอุปกรณ์/ชิ้นส่วน เพื่อทดแทน
2. เปลี่ยนอุปกรณ์ชิ้นส่วนที่เสียหาย
3. ซ่อมบำรุงวัสดุอุปกรณ์ที่เสียหาย
4. นำสื่อที่ได้สำรองข้อมูลไว้กลับมา Restore โดยเร็ว
5. ตรวจสอบระบบปฏิบัติการ ระบบฐานข้อมูล ตรวจสอบความถูกต้องของข้อมูลและ ระบบอื่น ๆ ที่เกี่ยวข้อง

ผู้รับผิดชอบ

1. ระดับนโยบาย

   ผู้บริหารเทคโนโลยีสารสนเทศระดับสูง ของหน่วย รับผิดชอบในการกำหนดนโยบาย ให้ข้อเสนอแนะ คำปรึกษา ตลอดจน ติดตาม กำกับดูแล ควบคุม ตรวจสอบ เจ้าหน้าที่ในระดับปฏิบัติ

2. ระดับปฏิบัติ

   เจ้าหน้าที่ผู้ดูแลระบบของหน่วย รับผิดชอบ กำกับ ดูแล การปฏิบัติงานของผู้ปฏิบัติ ศึกษา ทบทวน วางแผน ติดตาม การบริหารความเสี่ยง และรักษาความปลอดภัยระบบฐานข้อมูลและระบบเทคโนโลยีสารสนเทศ

การติดตามและรายงานผล

กำหนดให้เจ้าหน้าที่ผู้รับผิดชอบรายงานผลการดำเนินการหรือการตรวจสอบให้ผู้บังคับบัญชาทราบเป็นประจำ และให้รายงานการเกิดปัญหาและผลการแก้ไขให้ทราบในทันทีที่สามารถดำเนินการได้ ในทุกกรณีตามที่ระบุไว้

BANGKOK CRYSTAL	ชื่อเอกสาร แผนแก้ไขปัญหาระบบเทคโนโลยีสารสนเทศ - ฝ่ายส่งเสริมการลงทุน
จัดทำโดย	หมายเลขเอกสาร QD-B7-019
ทบทวนโดย	ครั้งที่แก้ไข 00
อนุมัติโดย	วันที่บังคับใช้ 01/05/21