WEALTH
Concept

# นโยบาย บริษัทหลักทรัพย์นายหน้าซื้อขายหน่วยลงทุน เวลธ์ คอนเซปท์ จำกัด
# แผนฉุกเฉิน (Business Continuity Plan)

## 1. วัตถุประสงค์

บริษัทหลักทรัพย์นายหน้าซื้อขายหน่วยลงทุน เวลธ์ คอนเซปท์ จำกัด ("บริษัทฯ") ได้ตระหนักถึงภัยต่างๆ ที่อาจเกิดขึ้น และอาจจะส่งผลกระทบต่อการปฏิบัติงานของบริษัทฯ ในช่วงระยะเวลาอันสั้นหรือในระยะยาวในหลายๆ ปัจจัย ประกอบด้วย

1.1 ปัจจัยภายในจากเหตุการณ์การขาดแคลนทรัพยากรบุคคล ไฟฟ้าดับ เครื่องมือเครื่องใช้ไม่มีหรือเสียหาย ชำรุด

1.2 ปัจจัยภายนอกซึ่งทำให้ไม่สามารถเข้าพื้นที่สำนักงานได้เนื่องจากเหตุการณ์การก่อการร้าย การจลาจล การชุมนุมทางการเมือง การปฏิวัติรัฐประหาร และเหตุการณ์ภัยทางธรรมชาติต่างๆ เช่น แผ่นดินไหว อัคคีภัย วาตภัย อุทกภัย หรือภัยจากโรคระบาด เป็นต้น หรือ

1.3 ระบบงานที่บริษัทใช้เป็นระบบงานหลักล่ม ใช้งานไม่ได้ เช่นระบบ Fund Connext ระบบ Streaming Fund+

1.4 ระบบงาน IT ภายใน (INTRA) บริษัทหยุดชะงัก หรือใช้งานไม่ได้

แผนฉุกเฉินนี้ ได้มีการปรับปรุงข้อมูลให้เป็นปัจจุบันและสื่อสารให้พนักงาน ทุกคนได้รับทราบ เพื่อให้มั่นใจว่าหากเกิดเหตุการณ์ขึ้น พนักงาน ที่มีความรับผิดชอบในเรื่องต่างๆ กัน จะสามารถปฏิบัติงานได้ทันท่วงทีโดยมีข้อมูลที่เพียงพอและเหมาะสมกับระยะเวลา เพื่อช่วยลดความเสี่ยงที่มีผลกระทบต่อการดำเนินงานของบริษัทฯ (Operation Risks) ภายใต้สถานการณ์ที่ไม่ปกติ สามารถช่วยบริษัทฯ แก้ไขปัญหา ในการติดต่อสื่อสารกับลูกค้า outsource และหน่วยงานที่กำกับดูแลบริษัท โดยดูแลและรับผิดชอบให้การติดต่อสื่อสาร และการดำเนินงานของบริษัท เป็นไปอย่างต่อเนื่อง หรือมีผลกระทบน้อยที่สุด

## 2. การเตรียมความพร้อมเพื่อรองรับเหตุฉุกเฉิน

2.1 การสำรวจข้อมูลที่สำคัญของฝ่ายงาน ข้อมูลสำคัญของบริษัท เช่น ใบอนุญาตประกอบธุรกิจ ใบสำคัญการจดทะเบียนบริษัท ใบจดทะเบียนภาษีมูลค่าเพิ่ม ข้อมูล บลจ.ซึ่งอยู่ในรูปแบบเอกสาร (Hard Copy) จะถูกสแกนและจัดเก็บ เป็น Soft File ของสำนักเลขานุการ ส่วนข้อมูลฝ่ายงานต่าง ๆ ได้แก่ ข้อมูล Customer Profile เอกสารการเปิดบัญชี ใบคำสั่งซื้อ/ขาย/สับเปลี่ยนหน่วยลงทุน เอกสารประกอบการรับ - จ่ายเงิน เอกสารสัญญาทุกฉบับ และเอกสารประกอบการตรวจสอบอื่นที่สำคัญ จัดเก็บตามวิธีการที่กำหนดไว้ในคู่มือปฏิบัติงานภายใน

2.2 รวบรวมข้อมูลด้านบุคลากรในบริษัทฯ ซึ่งครอบคลุมถึงบุคลากรในฝ่ายต่างๆ ตลอดจนรายชื่อบุคคลในครอบครัวของพนักงานที่จำเป็นต้องติดต่อฉุกเฉิน

2.3 ทุกฝ่ายงานจะต้องรวมรวมข้อมูลอื่นๆ ที่จำเป็น ซึ่งอาจต้องใช้ในกรณีฉุกเฉิน เช่น รายชื่อและเบอร์โทรศัพท์ของคู่ค้า บลจ. ผู้ให้บริการด้านต่างๆ เช่น ระบบโทรศัพท์ภายใน หรือ ผู้ประสานงานของ Regulator และบริการอื่นๆ ที่จำเป็น

2.4 การจัดการ การดำเนินงานและความพร้อมของทรัพยากรหากเกิดเหตุฉุกเฉิน ได้แก่ กรณีประสบภัยธรรมชาติ และกรณีทดแทนทรัพยากรที่ขาดแคลนบุคคล และหรืออุปกรณ์ใช้งาน ชำรุด และหยุดชะงัก ฝ่ายบุคคลและธุรการ รวบรวมและจัดทำข้อมูลด้านทรัพยากรบุคคลเพื่อแจ้งเหตุกรณีต่างๆ โดยให้ดำเนินการดังนี้

1) รายชื่อบุคคลในครอบครัวหรือเพื่อนสนิท กรณีแจ้งเหตุฉุกเฉินที่เกิดขึ้นกับพนักงาน

2) หมายเลขโทรศัพท์แจ้งเหตุฉุกเฉินด้านอาคารสถานที่ ให้แจ้งเจ้าหน้าที่ฝ่ายบริการทั่วไป หากติดต่อไม่ได้ให้ติดต่อฝ่ายอาคาร All Seasons Property Management Co.,Ltd. รายงานเหตุฉุกเฉินฝ่ายบริหารอาคาร หมายเลขโทรศัพท์ 02-654-3333

**3. ปัจจัยภายนอกที่ส่งผลให้ไม่สามารถเข้าพื้นที่ของบริษัทได้**

เนื่องจากเหตุจราจล การปฏิวัติ การชุมนุมทางการเมือง การขู่วางระเบิด การเกิดอัคคีภัย หรือภัยพิบัติทางธรรมชาติอื่นใด หรือภัยจากโรคระบาด กำหนดให้หัวหน้าของฝ่ายงานทำหน้าที่ประสานงานกับประธานเจ้าหน้าที่บริหารของบริษัทฯ เพื่อหารือหรือกำหนดแนวทางในทางปฏิบัติ โดยประธานเจ้าหน้าที่บริหารจะเป็นผู้สั่งการให้ปฏิบัติตามแผน BCP และแจ้งให้พนักงานทุกคนรับทราบถึงแนวทางปฏิบัติตนต่อไป การแจ้งอาจใช้วิธีการสื่อสารผ่านโทรศัพท์ email , Group Line พนักงานทุกคนสามารถปฏิบัติงานภายนอกสำนักงานได้ เนื่องจากบริษัทได้มีการสำรองข้อมูลเพื่อใช้ในการปฏิบัติงานไว้ในระบบ Cloud

**4. ปัจจัยภายนอกที่สำคัญ ได้แก่ ระบบงานที่บริษัทใช้เป็นระบบงานหลักล่ม ได้แก่ ระบบ Fund Connext ใช้งานไม่ได้ ให้ดำเนินการดังนี้**

4.1 กรณีที่ระบบ Fund connext ไม่สามารถใช้งานได้ ฝ่ายเทคโนโลยีสารสนเทศจะ email แจ้งไปยังเจ้าหน้าที่แนะนำการลงทุนทุกท่านทันที เพื่อให้เจ้าหน้าที่แนะนำการลงทุนแจ้งลูกค้าที่ประสงค์จะทำรายการว่า ระบบ Fund connext ไม่สามารถใช้งานได้

4.2 หากลูกค้ายังประสงค์ที่จะทำรายการซื้อ/ขาย/สับเปลี่ยนหน่วยลงทุน ให้เจ้าหน้าที่แนะนำการลงทุนสามารถให้บริการรับคำสั่งได้ 2 รูปแบบ ดังนี้

4.2.1 กรณีลูกค้ามีการลงนามในใบคำสั่งซื้อ/ขาย/สับเปลี่ยนหน่วยลงทุน

เจ้าหน้าที่แนะนำการลงทุนให้ลูกค้าลงนามในใบคำสั่งซื้อ/ขาย/สับเปลี่ยนหน่วยลงทุนจากนั้นดำเนินการจะส่งรูปถ่ายใบคำสั่ง และ Pay in Slip ให้เจ้าหน้าที่ฝ่ายสนับสนุนการขายผ่านทางไลน์/email โดยทันที เจ้าหน้าที่ฝ่ายสนับสนุนการขายดำเนินการตรวจสอบข้อมูลลูกค้าจากฐานข้อมูลลูกค้าที่ทาง ฝ่าย IT backup ไว้ และความถูกต้องครบถ้วนของเอกสาร ก่อนส่ง email ให้ฝ่ายปฏิบัติการหลักทรัพย์ เมื่อฝ่ายปฏิบัติการหลักทรัพย์ตรวจสอบข้อมูลว่าถูกต้องแล้วจึงดำเนินการส่งคำสั่งผ่านช่องทาง email ไปยัง บลจ. หรือการทำรายการผ่านระบบของ บลจ. (ถ้ามี) โดยฝ่ายปฏิบัติการหลักทรัพย์จะทำการกระทบยอดเงินโอนเงินเข้าบัญชีจองซื้อกับรายการคำสั่งซื้อของลูกค้า

4.2.2 กรณีลูกค้าส่งคำสั่งซื้อ/ขาย/สับเปลี่ยนหน่วยลงทุนทางโทรศัพท์

เจ้าหน้าที่แนะนำการลงทุนแจ้งเจ้าหน้าที่ฝ่ายสนับสนุนการขายว่าลูกค้ามีความประสงค์จะรายการซื้อ/ขาย/สับเปลี่ยนหน่วยลงทุนทางโทรศัพท์ โดยแจ้งผ่านระบบ email เจ้าหน้าที่ฝ่ายสนับสนุนการขายดำเนินการตรวจสอบข้อมูลลูกค้าจากฐานข้อมูลลูกค้าที่ทาง ฝ่าย IT backup ไว้ และความถูกต้องครบถ้วนของเอกสาร จากนั้นเจ้าหน้าที่ฝ่ายสนับสนุนการขายโทรศัพท์โทรไปหาเจ้าหน้าที่แนะนำการลงทุน และลูกค้า เพื่อทำการบันทึกเทปการสนทนา 3 สาย เจ้าหน้าที่ฝ่ายสนับสนุนการขายสรุปรายการคำสั่งเป็น Excel file พร้อมด้วย Pay in Slip แล้วส่ง email ให้ฝ่ายปฏิบัติการหลักทรัพย์ เมื่อฝ่ายปฏิบัติการ

หลักทรัพย์ตรวจสอบข้อมูลว่าถูกต้องแล้ว จะทำการส่งคำสั่งผ่านช่องทาง email ไปยัง บลจ. หรือทำรายการผ่านระบบของ บลจ. (ถ้ามี) โดยฝ่ายปฏิบัติการหลักทรัพย์จะทำการกระทบยอดเงินโอนเงินเข้าบัญชีจองซื้อกับรายการคำสั่งซื้อของลูกค้า

4.3 เมื่อสิ้นวัน ฝ่ายสนับสนุนการขาย และ ฝ่ายปฏิบัติการหลักทรัพย์จะมีการตรวจทานรายการซื้อ/ขาย/สับเปลี่ยนหน่วยลงทุนร่วมกัน และเมื่อข้อมูลที่ตรวจทานถูกต้องแล้ว ฝ่ายปฏิบัติการหลักทรัพย์จะมีการตรวจทานกับทาง บลจ. เพื่อเป็นการยืนยันรายการซื้อขายว่าเป็นไปตามที่ลูกค้าต้องการ

**5. การบริหารความต่อเนื่องทางธุรกิจในด้านความปลอดภัยสารสนเทศ**

บริษัทจัดให้มีขั้นตอน กระบวนการดำเนินการ และการควบคุมด้านความมั่นคงปลอดภัยของระบบสารสนเทศ เพื่อให้มั่นใจได้ว่ามีความสอดคล้องกับแผนบริหารความต่อเนื่องทางธุรกิจ จัดให้มีการรายงานสถานการณ์ที่เกิดขึ้นอย่างรวดเร็วและทันต่อเหตุการณ์ แจ้งต่อประธานเจ้าหน้าที่บริหาร โดยให้ดำเนินการดังนี้

- จัดทำแบบฟอร์มที่เป็นมาตรฐานเพื่อรองรับการรายงานสถานการณ์ และสร้างความเข้าใจให้กับผู้รายงานเกี่ยวกับการดำเนินการต่าง ๆ ที่จำเป็นในกรณีที่เกิดเหตุการณ์ทั้งนี้ เนื้อหาขั้นต่ำต้องประกอบด้วย วันเวลา เหตุการณ์ ผลกระทบที่คาดว่าจะเกิดขึ้น การดำเนินการแก้ไข ผลการแก้ไข ระยะเวลาในการแก้ไข สาเหตุที่เกิดปัญหา และแนวทางการป้องกันในอนาคต
- รายงานต่อประธานเจ้าหน้าที่บริหาร เมื่อทราบเหตุการณ์ที่อาจส่งผลกระทบต่อความมั่นคงปลอดภัย เช่น พบช่องโหว่ในการควบคุมความมั่นคงปลอดภัย (ineffective security control) เกิดเหตุการณ์ ที่อาจส่งผลกระทบต่อการรักษาความลับ (confidentiality) ความถูกต้องครบถ้วน (integrity) และสภาพพร้อมใช้งาน (availability) ของระบบสารสนเทศ ข้อผิดพลาดจากการปฏิบัติงาน (human errors) การบุกรุกด้านกายภาพ (breaches of physical security arrangements) การปฏิบัติงาน ที่ไม่เป็นไปตามนโยบายด้านการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ (non-compliances with policies) การเปลี่ยนแปลงระบบปฏิบัติการหรือชุดคำสั่งที่ควบคุมระบบงานโดยไม่ได้รับอนุญาต (uncontrolled system changes) การทำงานผิดพลาดของโปรแกรมและอุปกรณ์คอมพิวเตอร์ (malfunctions of software or hardware) และการเข้าถึงโดยไม่ได้รับอนุญาต (access violations)
- รายงานสำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์เมื่อมีเหตุการณ์ที่ส่งผลกระทบต่อระบบสารสนเทศที่มีความสำคัญ ประเภทดังต่อไปนี้
- ระบบหยุดชะงัก (system disruption)
- มีการบุกรุก เข้าถึง หรือใช้งานระบบโดยไม่ได้รับอนุญาต (system compromised)
- ส่งผลกระทบต่อชื่อเสียงของผู้ประกอบธุรกิจ (harm to reputation) เช่น ถูกปลอมแปลงหน้าเว็บไซต์ของบริษัท (website defacement) โดยให้รายงาน ดังนี้

  - รายงานทันทีเมื่อทราบเหตุการณ์โดยมีเนื้อหาครอบคลุมถึงวันเวลา ประเภทเหตุการณ์ และผลกระทบ ที่คาดว่าจะเกิดขึ้น ทั้งนี้ อาจแจ้งโดยวาจาหรือผ่านระบบรับส่งข้อความผ่านทางอิเล็กทรอนิกส์ (electronic messaging) ตามความเหมาะสม
  - รายงานภายในวันทำการถัดไปหลังทราบเหตุการณ์เป็นลายลักษณ์อักษร โดยมีเนื้อหาครอบคลุมถึงวันเวลา ประเภทเหตุการณ์ ผลกระทบที่เกิดขึ้น การดำเนินการแก้ไขปัญหาและความคืบหน้าในการแก้ไขปัญหา

- รายงานเมื่อเหตุการณ์ยุติหรือแก้ไขปัญหาแล้วเสร็จ เป็นลายลักษณ์อักษร โดยมีเนื้อหาครอบคลุมถึงวันเวลาประเภทเหตุการณ์ ผลกระทบที่เกิดขึ้น การดำเนินการแก้ไขปัญหา ผลการแก้ไขปัญหา ระยะเวลาในการแก้ไข สาเหตุที่เกิดปัญหาและแนวทางป้องกันในอนาคต

- แจ้งบุคคลในฝ่ายที่เกี่ยวข้อง เช่น แจ้งฝ่ายความมั่งคั่งเพื่อแจ้งต่อลูกค้า และตลาดหลักทรัพย์ รับทราบโดยไม่ชักช้า ในกรณีที่เหตุการณ์ส่งผลกระทบต่อบุคคลดังกล่าว

- จัดให้มีการรายงานความคืบหน้าในการบริหารจัดการสถานการณ์และผลการบริหารจัดการเป็นระยะ และเมื่อเหตุการณ์ยุติแล้ว

**6. การเตรียมพร้อมกรณีฉุกเฉินด้าน IT**

6.1 บริษัทฯ ได้เตรียมแผนฉุกเฉินสำหรับอุปกรณ์ต่างๆ ที่สามารถกู้ระบบคอมพิวเตอร์ได้เร็วที่สุดโดยการจัดหาอุปกรณ์สำรองตาม ข้อมูลระบบสำรอง ไว้เพื่อทดแทนทันที เมื่อระบบหลักมีปัญหา ทำให้โอกาสที่จะได้รับความเสียหายน้อยลง

6.2 ลำดับความสำคัญของระบบงาน และระยะเวลาในการกู้ระบบนับจากได้รับแจ้ง หรือตรวจสอบเจอปัญหา

| ลำดับ | ระบบงาน | ผู้รับผิดชอบ |
|---|---|---|
| 1 | ระบบ Internet | คุณรังสรรค์ มนัสมานะชัย |
| 2 | ระบบ Network | คุณรังสรรค์ มนัสมานะชัย |
| 3 | ระบบ FundConnext | คุณรังสรรค์ มนัสมานะชัย |
| 4 | ระบบ Streaming Fund+ | คุณรังสรรค์ มนัสมานะชัย |
| 5 | ระบบ email | คุณรังสรรค์ มนัสมานะชัย |
| 6 | ระบบ บัญชี | คุณรังสรรค์ มนัสมานะชัย |
| 7 | ระบบ BackOffice | คุณรังสรรค์ มนัสมานะชัย |

6.3 บริษัทฯ ได้มีการจัดทำและ Review แผน Call Out Tree อย่างน้อยปีละ **1** ครั้ง

6.4 บริษัทให้มีการกำหนดให้จัดเก็บหลักฐานในการบริหารจัดการ IT incident ไว้อย่างน้อย 2 ปี

เบอร์โทรศัพท์ที่ติดต่อได้

1. คุณรังสรรค์ มนัสมานะชัย เบอร์โทรศัพท์ 084 044 0555
2. คุณประกอบ อนันเอื้อ เบอร์โทรศัพท์ 094 851 1011

**<u>ผู้รับผิดชอบ: หัวหน้าฝ่าย IT</u>** มีข้อปฏิบัติ ดังนี้

1. เมื่อทราบปัญหาทาง หัวหน้าฝ่าย IT จะต้องรายงานแก่ประธานเจ้าหน้าที่บริหาร ถึงสาเหตุและวิธีการแก้ไขปัญหาตามแนวทางของแผนสำรองฉุกเฉินแต่ละกรณี (Call Out Tree)

2. ในกรณีที่จำเป็นต้องใช้แผนสำรองฉุกเฉินจะต้องดำเนินการทันทีที่ได้รับอนุมัติ

3. หลังจากที่เหตุการณ์ฉุกเฉินได้ผ่านไปแล้ว จะต้องนำระบบที่เป็นระบบงานจริง กลับมาใช้ตามปกติ

**<u>รายละเอียดความหมายและความสำคัญของระบบ</u>**

1. ความเสี่ยงสูง : หมายถึงระบบที่เมื่อเกิดเหตุขัดข้องบริษัทฯ จะไม่สามารถดำเนินธุรกิจต่อได้ และต้องได้รับการกู้คืนระบบอย่างเร็วที่สุด ได้แก่ระบบดังต่อไปนี้

a. ระบบซื้อขายหลักทรัพย์ หรือ หน่วยลงทุน

b. ระบบ Network ที่เชื่อมไปยังตลาดหลักทรัพย์ (Fund Connext/Streaming Fund+)

c. ระบบ Backoffice ที่ใช้สำหรับหลักทรัพย์

d. WEB Site หลักของ บริษัทฯ

2. ความเสี่ยงปานกลาง: หมายถึงระบบที่เมื่อเกิดเหตุขัดของบริษัท ฯ สามารถดำเนินธุรกิจต่อได้ แต่ต้องได้รับการรับการกู้คืนระบบภายใน 1 วัน เพราะอาจต้องมีการหางาน EOD (End of Day) ต่างๆ ได้แก่ ระบบดังต่อไปนี้

a. ระบบบัญชี

b. ระบบ File Server

c. ระบบ Network อื่น ๆ ที่ไม่ได้เชื่อมต่อกับตลาดหลักทรัพย์

d. ระบบ email

3. ความเสี่ยงต่ำ: หมายถึงระบบเมื่อเกิดเหตุขัดของบริษัท ฯ สามารถดำเนินธุรกิจต่อได้และผลกระทบต่ำ ได้แก่ระบบดังต่อไปนี้

a. Information Server

**<u>แผนสำรอง IT</u>**

บริษัทฯโดยผู้บริหารและฝ่าย IT จัดให้มีการประเมินความเสี่ยงของระบบงานต่างๆอย่างน้อยปีละ 1 ครั้ง โดยขั้นตอนเมื่อมีการประเมินแล้วต้องดำเนินการรองรับต่าง ๆ ตามรายละเอียดดังนี้

1. ระบบที่มีความเสี่ยงสูงต้องมีการสำรองทั้ง Hardware Software การ Setup Synchronize ระบบแบบ Real Time และติดตั้งระบบ Backup ที่ศูนย์สำรองพร้อมทั้งจัดให้มีการทดสอบระบบสำรองอย่างน้อยปีละ 1 ครั้ง

2. ระบบที่มีความเสี่ยงปานกลาง ต้องมีการสำรอง Hardware Software การ Setup ระบบ Backup แบบ Daily Routine และติดตั้งระบบไว้ที่ศูนย์สำรอง เพื่อให้พร้อมต่อการกู้คืนข้อมูลและจัดให้มีการทดสอบระบบสำรองอย่างน้อยปีละ 1 ครั้ง

3. ระบบที่มีความเสี่ยงต่ำต้องมีการสำรอง Hardware หรือ Software แล้วแต่ระบบนั้น ๆ และมีการสำรองข้อมูลเพื่อไว้ใช้กู้คืนกรณีมีเหตุการณ์

**รายละเอียดของ Recovery Point Objective**

การดำเนินการ RPO หมายถึงระยะเวลาในการนำระบบ Backup มาใช้งานโดยให้แบ่งแยกตามรายละเอียดความหมายและความสำคัญของระบบ ดังต่อไปนี้

1. ระบบที่มีความเสี่ยงสูง ต้องมีการทำ Synchronize ระดับ Application เพื่อให้สามารถดาเนินการทำงานได้ทันทีเมื่อต้องการใช้งานระบบ Backup

2. ระบบที่มีความเสี่ยงปานกลางให้ดำเนินการ Backup แบบ Daily โดยให้สามารถคืนข้อมูลย้อนหลังได้อย่างน้อย 1 วันทำการ

3. ระบบที่มีความเสี่ยงต่ำ สามารถดำเนินการติดตั้ง Server ใหม่และติดต่อผู้ให้บริการเพื่อน่าข้อมูลย้อนหลังมาติดตั้งใหม่

**รายละเอียดของ Recovery Time Objective**

การดำเนินการ RTO หมายถึงระยะเวลาในการนำระบบ Production ให้สามารถกลับมาใช้งานได้ตามปกติ โดยให้แบ่งแยกตาม รายละเอียดความหมายและความสำคัญของระบบดังต่อไปนี้

1. ระบบที่มีความเสี่ยงสูง ให้ดำเนินการทำ RTO ได้ทันทีภายหลังจากนอกเวลาทำการเช่น ช่วงเวลาตลาดฯปิดหรือระบบ Back office เมื่อทำการ EOD เรียบร้อยแล้ว

2. ระบบที่มีความเสี่ยงปานกลาง ให้ดำเนินการทำ RTO ได้ทันทีเมื่อสามารถแก้ไขระบบที่ Production เรียบร้อยแล้ว โดยต้องแจ้ง User หยุดใช้งานก่อนการนำ Production กลับมาทำงาน

3. ระบบที่มีความเสี่ยงต่ำ สามารถดำเนินการได้ทันทีเมื่อระบบ Production แก้ไขเรียบร้อย

. ระบบ Network และระบบ email

ผู้รับผิดชอบ : System Engineer

ระดับความเสี่ยง : ปานกลาง

ระยะเวลาในการดำเนินการเพื่อให้สามารถปฏิบัติงานที่ระบบ Backup ได้ : ไม่เกิน 30 นาที หรือกรณีนอกเวลาทำการสามารถดำเนินการได้โดยไม่ส่งผลกระทบต่อการทำงาน

นโยบายการดำเนินงาน : ฝ่าย IT จัดให้มีระบบสำรองและ Backup Link ทุกๆ Link ที่มีการใช้งานในบริษัทฯ

. ระบบเครื่องคอมพิวเตอร์ส่วนบุคคล

ผู้รับผิดชอบ : System Engineer

ระดับความเสี่ยง : ปานกลาง

นโยบายการดำเนินงาน : ฝ่าย IT ต้องมีการสำรองเครื่องคอมพิวเตอร์ให้พร้อมสำหรับพนักงานที่พบปัญหาการใช้งานความเสี่ยงที่ประเมิน

**การประเมินความเสี่ยง**

ฝ่าย IT ได้ทำการประเมินความเสี่ยง โดยแบ่งแยกตามสถานการณ์ต่างๆดังนี้

1. ความเสี่ยงจากภัยธรรมชาติ เช่น ไฟไหม้, น้ำท่วม, แผ่นดินไหว
2. ความเสี่ยงจากระบบ IT เช่น ระบบหลักที่ใช้งานมีปัญหา
3. ความเสี่ยงจากภัยคุกคามทาง IT เช่น Virus, Cyber Attack, ransomware
4. ความเสี่ยงจากสถานการณ์ฉุกเฉินพิเศษ เช่นการชุมนุม
5. ความเสี่ยงจากโรคระบาด

ในการประเมินความเสี่ยง ฝ่าย IT ต้องเป็นผู้แจ้งต่อประธานเจ้าหน้าที่บริหาร และเป็นผู้กำหนดถึงระบบการทำงาน โดยให้ปฏิบัติตามแนวทางดังต่อไปนี้

1. กรณีความเสี่ยงจากภัยธรรมชาติ ฝ่าย IT มีหน้าที่ประเมินการปฏิบัติงานดังนี้
   - ระบบไม่มีปัญหาแต่ไม่สามารถเข้าปฏิบัติงานที่อาคารได้ ให้ดำเนินการผ่านระบบ Internet
   - ระบบมีปัญหาและไม่สามารถเข้าปฏิบัติงานที่อาคารได้ ให้ดำเนินการผ่านระบบ Internet
2. ความเสี่ยงจากระบบของฝ่าย IT โดยให้ประเมินการทำงานดังนี้
   - ระบบมีปัญหาแต่พนักงานยังสามารถเข้าทำงานที่อาคารได้ปกติ ให้ดำเนินการใช้ระบบสำรอง ตามที่ระบบนั้นๆมีปัญหา และให้พนักงานเข้าทำงานที่อาคารตามปกติ
3. ความเสี่ยงจากภัยคุกคามทาง IT ฝ่าย IT มีหน้าที่ประเมินการปฏิบัติงานดังนี้
   - ฝ่าย IT ต้องทำการประเมินความเสียหายต่อระบบโดยรวมเกี่ยวกับผลกระทบทั้งหมด
   - รายงานสถานการณ์ต่อผู้บังคับบัญชาโดยเร่งด่วนที่สุด
   - รายงานสถานการณ์ให้ส่วนงานที่เกี่ยงข้องทราบ ได้แก่ Compliance, ประชาสัมพันธ์เพื่อฝ่ายต่างๆแจ้งกับหน่วยงานภายนอก
   - ติดต่อ Vendor ผู้ให้บริการระบบเพื่อหาวิธีจำกัดความเสียหายโดยเร็วที่สุด
   - ดำเนินการกู้คืนระบบตามที่ได้ทำการประเมินการกู้คืนไว้แล้ว
4. ความเสี่ยงจากสถานการณ์ฉุกเฉินพิเศษ ฝ่าย IT มีหน้าที่ประเมินการปฏิบัติงานดังนี้
   - ระบบไม่มีปัญหา แต่ไม่สามารถเข้าปฏิบัติงานที่อาคารได้ ให้ดำเนินการทำงานผ่านระบบ Internet
   - ระบบมีปัญหาและไม่สามารถเข้าปฏิบัติงานที่อาคารได้ให้ดำเนินการ Start ระบบที่ ศูนย์สำรอง และให้พนักงานทำงานผ่านระบบ Internet
5. ความเสี่ยงจากโรคระบาดฝ่าย IT มีหน้าที่ประเมินการปฏิบัติงานดังนี้
   - ระบบไม่มีปัญหา แต่ไม่สามารถเข้าปฏิบัติงานที่อาคารได้ ให้ดำเนินการทำงานผ่านระบบ Internet

**<u>การทดสอบแผนประจำปี</u>**

1. บริษัท กำหนดให้มีปรับปรุงแผนและรายชื่อผู้เกี่ยวข้องต่างๆ ภายหลังการทดสอบในแต่ละรอบ ซึ่งผู้เข้าร่วมการทดสสอบต้องแจ้งผลการทดสอบกลับมาที่ หัวหน้าฝ่าย IT จากนั้นฝ่าย IT ต้องมีการประเมินผลการทดสอบเพื่อแจ้งสรุปผล ต่อประธานเจ้าหน้าที่บริหารในขั้นถัดไป

2. แนะนำฝึกอบรมความพร้อมให้พนักงานเข้าใจและสามารถตอบสนองได้หากเกิดเหตุฉุกเฉิน

3. ศึกษาแผนผังของอาคารและเส้นทางประตูหนีไฟ และเข้าร่วมในการฝึกความพร้อมในการหนีภัยของอาคารทุกครั้ง

4. อบรม/ทำความเข้าใจร่วมกันระหว่างพนักงานทุกคนในฝ่ายงาน เพื่อให้เข้าใจในหน้าที่ของตนและเมื่อเกิดเหตุฉุกเฉินพนักงานทุกคนจะสามารถปฏิบัติตามแผนฉุกเฉินดังกล่าวได้อย่างมีประสิทธิภาพ

5. จัดให้มีการทดสอบแผนฉุกเฉิน เป็นประจำอย่างน้อยปีละ 1 ครั้ง

6. ให้มีการทบทวนแผนฉุกเฉิน เป็นประจำอย่างน้อยปีละ 1 ครั้ง เพื่อจัดทำข้อมูลให้เป็นปัจจุบัน

นโยบายฉบับนี้ให้มีผลบังคับตั้งแต่วันที่ 1 มีนาคม 2567 เป็นต้นไป

.....

(นายเจษฎา ยงพิทยาพงศ์ - ประธานเจ้าหน้าที่บริหาร)

| | | |
|---|---|---|
| จัดทำครั้งที่ 1 | อนุมัติโดยมติที่ประชุมคณะกรรมการบริษัท ครั้งที่ 2/2565 | วันที่ 8 สิงหาคม 2565 |
| จัดทำครั้งที่ 2 | อนุมัติโดยมติที่ประชุมคณะกรรมการบริษัท ครั้งที่ 1/2567 | วันที่ 20 กุมภาพันธ์ 2567 |