สำนักงานคณะกรรมการกำกับและส่งเสริม
การประกอบธุรกิจประกันภัย(คปภ.)
Office of Insurance Commission

แบบสอบถาม
เรื่อง แผนรองรับการดำเนินธุรกิจอย่างต่อเนื่องของบริษัทประกันภัย (Business Continuity Plan) และแผนรับมือภัยคุกคามทางไซเบอร์ (Incident Response Plan)

ตามที่สำนักงาน คปภ. ได้ออกแนวทางปฏิบัติ เรื่อง การบริหารความต่อเนื่องทางธุรกิจ (Business Continuity Management) และการจัดทำแผนรองรับการดำเนินธุรกิจอย่างต่อเนื่อง (Business Continuity Plan) เมื่อปี 2555 โดยแนวทางปฏิบัติฉบับดังกล่าวได้พัฒนาและกำหนดหลักเกณฑ์ภายใต้บริบทการดำเนินธุรกิจและสถานการณ์ของประเทศในขณะนั้น เช่น น้ำท่วม สถานการณ์ความไม่สงบทางการเมือง เป็นต้น แต่เนื่องจากปัจจุบันสภาพแวดล้อมในการดำเนินธุรกิจมีการเปลี่ยนแปลงจากในอดีต บริษัทได้นำเทคโนโลยีและพัฒนานวัตกรรมต่างๆ ขึ้นมาเป็นองค์ประกอบสำคัญในการดำเนินธุรกิจ ทั้งในด้านการพัฒนาผลิตภัณฑ์และการให้บริการลูกค้า ทำให้ความเสี่ยงหรือเหตุการณ์ที่จะส่งผลกระทบให้ธุรกิจเกิดการหยุดชะงักมีรูปแบบที่เปลี่ยนไป เช่น การถูกโจมตีทางไซเบอร์ในรูปแบบต่างๆ เป็นต้น ดังนั้น เพื่อให้แนวทางการกำกับดูแลเรื่องการดำเนินธุรกิจอย่างต่อเนื่องของบริษัทประกันภัยสอดคล้องกับบริบทและรูปแบบในการดำเนินธุรกิจในปัจจุบัน สำนักงาน คปภ. จึงได้ดำเนินการทบทวนแนวทางปฏิบัติเรื่อง BCM & BCP เพื่อปรับปรุงหลักเกณฑ์หรือข้อกำหนดต่างๆ ในแนวปฏิบัติให้เหมาะสมสอดคล้องกับสภาพแวดล้อมในการดำเนินธุรกิจและความเสี่ยงที่จะส่งผลให้การดำเนินงานของบริษัทเกิดการหยุดชะงัก

แบบสอบถาม เรื่อง แผนรองรับการดำเนินธุรกิจอย่างต่อเนื่องของบริษัทประกันภัย (Business Continuity Plan) และแผนรับมือภัยคุกคามทางไซเบอร์ (Incident Response Plan) จัดทำขึ้นโดยมีวัตถุประสงค์

1. เพื่อศึกษาและทบทวนแนวทางปฏิบัติเรื่อง BCM & BCP ของสำนักงาน คปภ. ในปัจจุบันให้สอดคล้องกับบริบทในการดำเนินธุรกิจและความเสี่ยง โดยจะนำข้อมูลที่ได้จากการสำรวจมาประกอบการพิจารณายกระดับและปรับปรุงแก้ไขแนวทางปฏิบัติเรื่อง BCM & BCP ให้มีความครอบคลุมแผนการตอบสนองต่อภัยคุกคามทางไซเบอร์ (Incident Response Plan)

2. เพื่อให้สำนักงาน คปภ. ทราบถึงแนวทางและระดับความพร้อมในการรับมือและตอบสนองต่อภัยคุกคามทางไซเบอร์ในทางปฏิบัติของบริษัทในปัจจุบัน

ทั้งนี้ ข้อมูลที่ท่านตอบมาในแบบสอบถามฉบับนี้ จะนำมาเป็นองค์ประกอบสำคัญในการพิจารณากำหนดแนวทางปฏิบัติเรื่อง แผนรองรับการดำเนินธุรกิจอย่างต่อเนื่องของบริษัทประกันภัย (Business Continuity Plan) และแผนรับมือภัยคุกคามทางไซเบอร์ (Incident Response Plan) อย่างเป็นนัยสำคัญ เพื่อให้กฎระเบียบที่สำนักงาน คปภ. จะดำเนินการพัฒนาต่อไปนั้นสอดคล้องกับบริบทในการดำเนินธุรกิจในปัจจุบัน และสามารถนำไปปรับใช้ให้เกิดการปฏิบัติอย่างเหมาะสมเพื่อสร้างความมั่นคงปลอดภัยและความเชื่อมั่นให้ผู้เอาประกันภัยและประชาชนต่อไป

สำนักงาน คปภ. จึงขอความร่วมมือท่านในการให้ข้อมูลตอบแบบสอบถามภายในวันศุกร์ที่ 17 มกราคม 2563 ทั้งนี้ ข้อมูลดังกล่าวจะถูกเก็บรักษาเป็นความลับ และจะใช้เพื่อประกอบการพิจารณาทบทวน

ปรับปรุงแนวทางปฏิบัติเรื่อง แผนรองรับการดำเนินธุรกิจอย่างต่อเนื่องของบริษัทประกันภัย (Business Continuity Plan) และแผนรับมือภัยคุกคามทางไซเบอร์ (Incident Response Plan) เท่านั้น

**** สำนักงาน คปภ. ขอขอบคุณในความร่วมมือการให้ข้อมูลของท่านล่วงหน้า ณ โอกาสนี้ ****

<u>คำอธิบาย</u>

แบบสอบถามฉบับนี้ ประกอบด้วย 4 ส่วน ดังนี้

ส่วนที่ 1 : ข้อมูลผู้ตอบแบบสอบถาม

ส่วนที่ 2 : แนวทางในการกำหนดนโยบายแผนรองรับการดำเนินธุรกิจอย่างต่อเนื่อง

ส่วนที่ 3 : นโยบายและมาตรการในการรับมือภัยคุกคามทางไซเบอร์

ส่วนที่ 4 : ข้อเสนอแนะอื่นๆ

คำนิยามเพื่อใช้ประกอบการตอบแบบสอบถาม

คำศัพท์	ความหมาย
ภัยคุกคามทางไซเบอร์	การกระทำหรือการดำเนินการใดๆ โดยมิชอบ โดยใช้คอมพิวเตอร์หรือระบบคอมพิวเตอร์หรือโปรแกรมไม่พึงประสงค์โดยมุ่งหมายให้เกิดการประทุษร้ายต่อระบบคอมพิวเตอร์ ข้อมูลคอมพิวเตอร์ หรือข้อมูลอื่นที่เกี่ยวข้อง และเป็นภยันตรายที่ใกล้จะถึง ที่จะก่อให้เกิดความเสียหายหรือส่งผลกระทบต่อการทำงานของคอมพิวเตอร์ ระบบคอมพิวเตอร์ หรือข้อมูลอื่นที่เกี่ยวข้อง
ระยะเวลาการหยุดชะงักที่ยอมได้สูงสุด(Maximum Tolerable Period of Disruption : MTPD)	ระยะเวลาที่ระบบหยุดชะงักที่ยอมรับได้สูงสุดหากเกินกำหนดเวลานี้แล้วจะไม่สามารถทำให้ธุรกิจกลับคืนสู่สภาพปกติได้
ระยะเวลาเป้าหมายในการฟื้นคืนสภาพ (Recovery Time Objective : RTO)	ระยะเวลาเป้าหมายที่ใช้ในการดำเนินการเพื่อให้กระบวนการกลับคืนสู่สภาพปกติหลังเกิดเหตุการณ์
ระยะเวลาสูงสุดที่ยอมให้ข้อมูลเสียหาย (Recovery Point Objective : RPO)	จุดเป้าหมายเวลาที่ข้อมูลจะได้ได้รับการกู้กลับคืนมา เพื่อให้กิจกรรมเดินหน้าต่อไปได้ หรือ สามารถยอมรับการสูญหายของข้อมูลได้เท่าไหร่
การบริหารความต่อเนื่องในการดำเนินธุรกิจ (Business Continuity Management : BCM)	แนวทางในการกำหนดนโยบาย มาตรฐาน และกระบวนการทำงานของทั้งบริษัท เพื่อให้มั่นใจว่ากรณีที่มีเหตุการณ์ที่ทำให้การปฏิบัติงานตามปกติเกิดการหยุดชะงัก ระบบงานที่สำคัญจะยังสามารถดำเนินการได้อย่างต่อเนื่องหรือกลับมาดำเนินการได้ในเวลาที่เหมาะสม
แผนรองรับการดำเนินธุรกิจอย่างต่อเนื่อง (Business Continuity Plan : BCP)	แผนงานที่เป็นลายลักษณ์อักษรที่กำหนดขั้นตอน และกระบวนการในการทำงานในการเรียกคืนการดำเนินงานให้กลับสู่ภาวะปกติ เพื่อให้ธุรกิจสามารถดำเนินการได้อย่างต่อเนื่อง เมื่อเกิดเหตุการณ์ดำเนินการหยุดชะงัก
แผนการตอบสนองต่อภัยคุกคามทางไซเบอร์ (Incident Response Plan : IRP)	แผนงานที่เป็นลายลักษณ์อักษรที่กำหนดถึงวิธีปฏิบัติเพื่อตอบสนองเมื่อเกิดเหตุภัยคุกคามทางไซเบอร์
แผนการเรียกคืนการดำเนินงานให้กลับสู่ภาวะปกติ (Business Recovery Plan : BRP หรือ Disaster Recovery Plan)	แผนงานที่เป็นลายลักษณ์อักษร ที่เตรียมไว้ในการกู้ระบบในกรณีที่ระบบล่ม ช่วยให้สามารถกู้คืนระบบและการทำงานกลับคืนสู่ปกติ
การวิเคราะห์ผลกระทบทางธุรกิจ (Business Impact Analysis : BIA)	การวิเคราะห์และวัดผลกระทบทางธุรกิจหรือความสูญเสียทางธุรกิจที่เกิดจากการหยุดชะงักของการดำเนินธุรกิจ
การฝึกซ้อมแบบ Table Top Exercise	การฝึกซ้อมรับมือภัยคุกคามทางไซเบอร์ โดยการจำลอง สถานการณ์การถูกโจมตีทางไซเบอร์ ซึ่งเน้นการทดสอบการปฏิบัติตามกระบวนการและแผนต่างๆ ตลอดจนวิธีการสื่อสาร การรายงาน การเรียกประชุม และสั่งการในแต่ละสถานการณ์ โดยไม่ได้ลงมือปฏิบัติจริงในเชิงเทคนิค แต่ผู้เข้าร่วมจะตอบ

	คำถาม แสดงความเห็น และดำเนินการต่างๆ ตามสถานการณ์ที่กำหนด เพื่อสร้างความเข้าใจเกี่ยวกับการรับมือกับเหตุการณ์ภัยคุกคามทางไซเบอร์
ระบบจำลองยุทธทางไซเบอร์ (Cyber Ranges)	เป็นฝึกบุคลากรด้านความมั่นคงปลอดภัยไซเบอร์ในสถานการณ์จำลองเสมือนจริง เพื่อให้ทีมรักษาความมั่นคงปลอดภัยและพนักงานขององค์กรได้ฝึกซ้อมการโจมตีและรับมือกับภัยคุกคามไซเบอร์รูปแบบต่างๆ

ส่วนที่ 1

ข้อมูลผู้ตอบแบบสอบถาม

1. ชื่อบริษัท_____

2. ชื่อผู้ตอบแบบสอบถาม_____

   ตำแหน่ง_____

3. Email _____

4. เบอร์โทรศัพท์ _____

ส่วนที่ 2

แนวทางในการกำหนดนโยบายแผนรองรับการดำเนินธุรกิจอย่างต่อเนื่อง

1. บริษัทมีแผนรองรับการดำเนินธุรกิจอย่างต่อเนื่อง (Business Continuity Plan: BCP Plan) หรือไม่

☐ มี และรองรับในกรณีดังต่อไปนี้ (ตอบได้มากกว่า 1 ข้อ)

☐ ภัยคุกคามทางไซเบอร์

☐ สถานการณ์ความไม่สงบทางการเมือง / เหตุการณ์จลาจล

☐ ข่าวลือ

☐ ภัยพิบัติ (ไฟไหม้ น้ำท่วม เป็นต้น)

☐ การประท้วงของพนักงาน

☐ อื่นๆ (โปรดระบุ) _____

☐ ไม่มี (ถ้าไม่มี บริษัทมีแผนในการดำเนินการอย่างไรบ้าง โปรดอธิบายโดยย่อ) _____

_____

_____

2. ในปัจจุบันบริษัทมีการกำหนดผู้มีหน้าที่ประกาศใช้แผน BCP ของบริษัทหรือไม่ (ตอบได้มากกว่า 1 ข้อ)

☐ มี : BCP สำหรับภัยคุกคามทางไซเบอร์ (โปรดระบุตำแหน่ง)_____

☐ มี : BCP สำหรับเหตุการณ์อื่นๆ (โปรดระบุตำแหน่ง)_____

☐ ยังไม่ได้กำหนดชัดเจน เนื่องจาก_____

3. บริษัทมีการกำหนดเจ้าหน้าที่ผู้ประสานงานกับ คปภ. ในกรณีที่บริษัทประกาศใช้ BCP หรือไม่

☐ มี (โปรดระบุตำแหน่ง) _____ ☐ ไม่มี

4. การสื่อสารภายในบริษัท

4.1 เมื่อเกิดเหตุการณ์ผิดปกติที่อาจส่งผลกระทบทำให้ธุรกิจหยุดชะงัก บริษัทมีการกำหนดกระบวนการสื่อสารภายในเพื่อแจ้งเตือนเกี่ยวกับเหตุการณ์ความผิดปกติที่เกิดขึ้นให้พนักงานทุกคนรับทราบ หรือไม่

☐ มี และใช้วิธีการสื่อสารดังต่อไปนี้ (ตอบได้มากกว่า 1 ข้อ)

☐ SMS

☐ Email

☐ Line/Messenger/WhatsApp/WeChat

☐ อื่นๆ (โปรดระบุ) _____

☐ ไม่มี

4.2 เมื่อมีการประกาศใช้แผน BCP บริษัทมีการกำหนดกระบวนการสื่อสารภายในบริษัทที่ชัดเจน หรือไม่

☐ มี และใช้วิธีการสื่อสารดังต่อไปนี้ (ตอบได้มากกว่า 1 ข้อ)

☐ SMS

☐ Email

☐ Line/Messenger/WhatsApp/WeChat

☐ อื่นๆ (โปรดระบุ) _____

☐ ไม่มี

4.3 บริษัทมีการจัดทำผังการติดต่อพนักงาน (Call Tree) หรือไม่

☐ มี ☐ ไม่มี

5. บริษัทมีนโยบายการประชาสัมพันธ์ให้กับผู้เอาประกันภัยและผู้มีส่วนได้เสียทราบเมื่อบริษัทมีการประกาศใช้แผน BCP หรือไม่

☐ มีนโยบายและครอบคลุมกรณีเหตุการณ์ภัยคุกคามทางไซเบอร์

☐ มีนโยบายแต่ไม่ครอบคลุมกรณีเหตุการณ์ภัยคุกคามทางไซเบอร์

☐ ไม่มี

6. บริษัทมีการกำหนดแนวทางปฏิบัติของพนักงานตามแผน BCP เพื่อให้บริษัทสามารถดำเนินงานสำคัญได้อย่างต่อเนื่อง หรือไม่

☐ มี ☐ ไม่มี

6.1 ในกรณีที่มีการกำหนดแนวทางปฏิบัติ โดยครอบคลุมในเรื่องดังต่อไปนี้ (ตอบได้มากกว่า 1 ข้อ)

☐ หน้าที่และความรับผิดชอบของผู้ปฏิบัติงานแต่ละตำแหน่งอย่างชัดเจน

☐ รายละเอียดวิธีปฏิบัติงานที่ต้องปฏิบัติตาม

☐ อื่นๆ (โปรดระบุ)_____

7. การวิเคราะห์และประเมินสถานการณ์ที่มีผลกระทบต่อการหยุดชะงักของการดำเนินงาน (Business Impact Analysis)

7.1 บริษัทมีการทำ Business Impact Analysis หรือไม่

☐ มี ☐ ไม่มี

7.1.1 ในกรณีที่มีการทำ Business Impact Analysis บริษัทได้คำนึงถึงเหตุการณ์ภัยคุกคามทางไซเบอร์หรือไม่

☐ มี ☐ ไม่มี

7.2 ในการจัดทำ Business Impact Analysis ของบริษัท มีการวิเคราะห์ปัจจัยดังต่อไปนี้หรือไม่ (ตอบได้มากกว่า 1 ข้อ)

☐ การกำหนดระยะเวลาหยุดดำเนินงานสูงสุดที่ยอมรับได้ของระบบงานต่างๆ (Maximum Tolerable Period of Disruption – MTPD)

☐ ระยะเวลาสูงสุดที่ยอมให้ข้อมูลเสียหาย (Recovery Point Objectives)

☐ ระยะเวลาเป้าหมายในการฟื้นคืนสภาพ (Recovery Time Objectives)

☐ การกำหนดลำดับความสำคัญของระบบงานและลำดับการกู้คืนระบบงาน

☐ อื่นๆ (โปรดระบุ) _____

8. กรณีที่ไม่สามารถเข้าทำงานในสำนักงาน หรือใช้เครื่องคอมพิวเตอร์และระบบงานสำคัญเพื่อปฏิบัติงานได้ บริษัทมีศูนย์ปฏิบัติงานสำรอง (Alternate Sites) หรือไม่ (ตอบได้มากกว่า 1 ข้อ)

☐ มีเป็นแบบ Hot site ☐ มีเป็นแบบ Cold site

☐ มีเป็นแบบ Warm site ☐ ไม่มี

9. ระยะห่างระหว่างสำนักงานใหญ่และศูนย์ปฏิบัติงานสำรองประมาณ (ระบุเป็นตัวเลข) กิโลเมตร

10. ศูนย์ปฏิบัติงานสำรองใช้ระบบสาธารณูปโภค(ระบบไฟฟ้า, การประปา, ระบบโทรคมนาคม และเส้นทางคมนาคม) ที่แยกออกจากสำนักงานใหญ่หรือไม่

☐ แยกออกจากกัน ☐ ไม่แยกออกจากกัน

11. ในกรณีที่ประกาศใช้ BCP แล้ว ศูนย์รับแจ้งเหตุเคลม/ศูนย์บริการลูกค้า ของบริษัทสามารถดำเนินการได้หรือไม่

☐ สามารถดำเนินการได้

☐ ไม่สามารถดำเนินการได้ เนื่องจาก_____

12. บริษัทมีแนวทางในการสำรองข้อมูล (Backup System) อย่างไร (ตอบได้มากกว่า 1 ข้อ)

☐ มีศูนย์สำรองข้อมูลจำนวน (ระบุเป็นตัวเลข) แห่ง สำหรับข้อมูลดังต่อไปนี้

- ☐ ข้อมูลลูกค้า
- ☐ ข้อมูลทางธุรกิจ
- ☐ ข้อมูลผลิตภัณฑ์และบริการ
- ☐ อื่นๆ (โปรดระบุ) _____

ระยะห่างจากสำนักงานใหญ่ประมาณ (ระบุเป็นตัวเลข) กิโลเมตร ความถี่ในการสำรองข้อมูล (ระบุเป็นตัวเลข) / (ระบุเป็นหน่วยเวลา เช่น ชั่วโมง วัน เดือน ฯลฯ)

☐ มีการสำรองข้อมูลผ่านระบบ Cloud สำหรับข้อมูลดังต่อไปนี้

- ☐ ข้อมูลลูกค้า
- ☐ ข้อมูลทางธุรกิจ
- ☐ ข้อมูลผลิตภัณฑ์และบริการ
- ☐ อื่นๆ (โปรดระบุ) _____

ความถี่ในการสำรองข้อมูล (ระบุเป็นตัวเลข) / (ระบุเป็นหน่วยเวลา เช่น ชั่วโมง วัน เดือน ฯลฯ)

☐ ไม่มี (ถ้าไม่มี บริษัทมีการสำรองข้อมูลอย่างไร โปรดอธิบายโดยย่อ) _____

_____

_____

13. บริษัทจัดให้มีการฝึกอบรมแก่พนักงานทุกคนเกี่ยวกับ BCPและแนวทางในการปฏิบัติหรือไม่

☐ มี โปรดระบุความถี่ (ระบุเป็นตัวเลข) ครั้ง/ปี

☐ ไม่มี เนื่องจาก_____

_____

14. บริษัทจัดให้มีการทดสอบแผน BCP หรือไม่

☐ มี โปรดระบุความถี่ (ระบุเป็นตัวเลข) ครั้ง/ปี

☐ ไม่มี เนื่องจาก_____

_____

15. บริษัทมีการกำหนดแผนการเรียกคืนการดำเนินงานให้กลับสู่ภาวะปกติ (Business Recovery Plan) หรือไม่

☐ มี ☐ ไม่มี

<u>กรณีบริษัทมี</u>การกำหนดแผนการเรียกคืนการดำเนินงานให้กลับสู่ภาวะปกติ (Business Recovery Plan) บริษัทได้กำหนดเรื่องดังต่อไปนี้ในแผนฯ หรือไม่

15.1 มีการกำหนดระยะเวลาการกลับมาดำเนินงานตามปกติ (RTO) ของระบบ Claim หรือไม่

☐ มี โปรดระบุ RTO <u>(ระบุเป็นตัวเลขตามด้วยหน่วยเวลา)</u> ☐ ไม่มี

15.2 มีการทดสอบ Business Recovery Plan หรือไม่

☐ มี โปรดระบุความถี่ _____ครั้ง/ปี

☐ ไม่มี

16. บริษัทมีการติดตามและทบทวนนโยบายที่เกี่ยวข้องกับการดำเนินธุรกิจอย่างต่อเนื่องหรือไม่

☐ มี โปรดระบุความถี่ _____ครั้ง/ปี ☐ ไม่มี

ส่วนที่ 3

แผนและมาตรการในการรับมือภัยคุกคามทางไซเบอร์

17. บริษัทมี Incident Response Plan สำหรับภัยคุกคามทางไซเบอร์ หรือไม่

☐ มี และรองรับในกรณีดังต่อไปนี้ (ตอบได้มากกว่า 1 ข้อ)

- ☐ Denial of Service & Distributed Denial of Service (DoS&DDoS)
- ☐ Session Hijacking and Man-in-the-Middle Attacks
- ☐ Phishing
- ☐ SQL Injection Attack
- ☐ Cross-Site Scripting (XSS)
- ☐ Malware
- ☐ Ransomware
- ☐ Insider Threat
- ☐ Credential Reuse
- ☐ Botnets
- ☐ อื่นๆ (โปรดระบุ) _____

☐ ไม่มี (โปรดอธิบายโดยย่อว่าบริษัทมีแผนในการดำเนินการอย่างไรบ้าง) _____

_____

_____

17.1 กรณีที่บริษัทมีการกำหนด Incident Response Plan สำหรับภัยคุกคามทางไซเบอร์ มีบุคคลหรือหน่วยงานใดบ้างที่มีส่วนเกี่ยวข้องกับกระบวนการนี้ (ตอบได้มากกว่า 1 ข้อ)

- ☐ คณะกรรมการบริษัท (Board of Directors)
- ☐ คณะผู้บริหาร (Executive Managements)
- ☐ ฝ่ายเทคโนโลยีสารสนเทศ (IT)
- ☐ ฝ่ายบริหารความเสี่ยง (Risk Management)
- ☐ ฝ่ายกำกับการปฏิบัติตามขั้นตอนทางกฎหมาย (Legal & Compliance)
- ☐ ฝ่ายตรวจสอบภายใน (Internal Audit)
- ☐ ฝ่ายทรัพยากรบุคคล (Human Resources)
- ☐ อื่นๆ (โปรดระบุ)_____

18. บริษัทมีบุคลากรที่ทำหน้าที่เฝ้าระวังและ/หรือรับมือเหตุภัยคุกคามทางไซเบอร์ หรือไม่ (เช่น Cyber security response team, Security operation center, etc.) (ตอบได้มากกว่า 1 ข้อ)

- ☐ มี โดยเป็นพนักงานของบริษัทเอง (โปรดระบุจำนวนคนเป็นตัวเลข) ☐ ไม่มี
- ☐ มี โดยเป็นพนักงาน Outsource (โปรดระบุจำนวนคนเป็นตัวเลข)

18.1 พนักงานของบริษัทที่เฝ้าระวังและ/หรือรับมือเหตุภัยคุกคามทางไซเบอร์ สามารถทำหน้าที่ใดดังต่อไปนี้ (ตอบได้มากกว่า 1 ข้อ)

- ☐ ตรวจจับภัยคุกคามทางไซเบอร์
- ☐ รับมือและตอบสนองเมื่อเกิดเหตุภัยคุกคามทางไซเบอร์
- ☐ สำรองและกู้คืนข้อมูลที่สูญหาย
- ☐ จัดการปิดช่องโหว่ที่ถูกโจมตีทางไซเบอร์
- ☐ สืบค้นต้นทางของการโจมตีทางไซเบอร์
- ☐ อื่นๆ (โปรดระบุ) _____

18.2 Outsource ของบริษัทที่เฝ้าระวังและ/หรือรับมือเหตุภัยคุกคามทางไซเบอร์ สามารถทำหน้าที่ใดดังต่อไปนี้ (ตอบได้มากกว่า 1 ข้อ)

- ☐ ตรวจจับภัยคุกคามทางไซเบอร์
- ☐ รับมือและตอบสนองเมื่อเกิดเหตุภัยคุกคามทางไซเบอร์
- ☐ สำรองและกู้คืนข้อมูลที่สูญหาย
- ☐ จัดการปิดช่องโหว่ที่ถูกโจมตีทางไซเบอร์
- ☐ สืบค้นต้นทางของการโจมตีทางไซเบอร์
- ☐ อื่นๆ (โปรดระบุ) _____

18.3 กรณีที่บริษัทมีการใช้บริการจากผู้ให้บริการภายนอก (Outsource) ในการเฝ้าระวังและ/หรือรับมือเหตุภัยคุกคามทางไซเบอร์ บริษัทมีการประเมินความเสี่ยงและผลกระทบจากผู้ให้บริการจากภายนอก หรือไม่

☐ มี ☐ ไม่มี

18.4 กรณีที่บริษัทมีการใช้บริการจากผู้ให้บริการภายนอก (Outsource) ในการเฝ้าระวังและ/หรือรับมือเหตุภัยคุกคามทางไซเบอร์ บริษัทได้ทำการตรวจสอบและประเมินผลการทำงานของผู้ให้บริการจากภายนอกหรือไม่

☐ มี ☐ ไม่มี

19. การเก็บข้อมูลการจราจรทางคอมพิวเตอร์และเฝ้าระวังตรวจสอบภัยคุกคามทางไซเบอร์ (Logging & Monitoring)

19.1 บริษัทมีการเฝ้าระวังตรวจสอบเครือข่ายจากภัยคุกคามทางไซเบอร์ หรือไม่

- ☐ มี (โปรดระบุระยะเวลา)
  - ☐ ตลอดเวลา (24/7)
  - ☐ อื่นๆ (โปรดระบุ) _____
- ☐ ไม่มี เนื่องจาก _____

19.2 บริษัทมีการเก็บ Log ประเภทใดบ้าง (สามารถตอบได้มากกว่า 1 ข้อ)

☐ ข้อมูลการเข้าถึงพื้นที่หวงห้าม (physical access log)

☐ ข้อมูลการเข้าถึงระบบปฏิบัติการฐานข้อมูลและระบบเครือข่ายคอมพิวเตอร์(authentication log)

☐ ข้อมูลการเข้าถึงและใช้งานระบบสารสนเทศ (application log)

☐ ข้อมูลการใช้งานอินเทอร์เน็ตผ่านระบบเครือข่ายคอมพิวเตอร์ภายในของผู้ประกอบธุรกิจ (internet access log)

☐ ข้อมูลการใช้งานแฟ้มข้อมูล (audit log)

☐ ข้อมูลการบริหาร (event log) ระบบปฏิบัติการ และ network firewall

☐ ข้อมูลจราจรคอมพิวเตอร์ของ network firewall (network firewall log)

☐ ข้อมูลการจัดการบริหารข้อมูล (database log)

☐ อื่นๆ (โปรดระบุ)_____

☐ ไม่มีการเก็บ Log ข้อมูลเนื่องจาก (โปรดระบุ)_____

19.2.1 กรณีมีการเก็บ Log ข้อมูล นำมาใช้ประโยชน์อะไรบ้าง (สามารถตอบได้มากกว่า 1 ข้อ)

☐ ใช้ในการตรวจสอบสถานะ การทำงานของระบบสารสนเทศ

☐ ใช้ในการสืบค้นหาตัวผู้กระทำผิดทางคอมพิวเตอร์

☐ มีการจัดเก็บแต่ยังไม่มีการดำเนินการใดๆ

☐ อื่นๆ (โปรดระบุ) _____

19.3 บริษัทมีการติดตามตรวจสอบภัยคุกคามทางไซเบอร์และเทคโนโลยีสารสนเทศ ทางกายภาพ (Physical Monitoring) หรือไม่ (เช่น การติดตั้งกล้องวงจรปิดในห้อง Server)

☐ มี ☐ ไม่มี

20. บริษัทมีการแบ่งปันข้อมูลข่าวสารภัยคุกคามทางไซเบอร์ กับหน่วยงานหรือบริษัทอื่น หรือไม่

☐ มี และได้ทำการแบ่งปันข้อมูลข่าวสารกับหน่วยงานและบริษัท ดังต่อไปนี้ (ตอบได้มากกว่า 1 ข้อ)

- ☐ บริษัทในเครือ
- ☐ Thai Insurance Computer Emergency Response Team (TI-CERT)
- ☐ อื่นๆ (โปรดระบุ) _____

☐ ไม่มี

21. Testing, Training & Exercise ภัยคุกคามทางไซเบอร์

21.1 บริษัทมีการทดสอบ Incident Response สำหรับภัยคุกคามทางไซเบอร์ หรือไม่ (ตอบได้มากกว่า 1 ข้อ)

☐ มี และทดสอบในรูปแบบต่อไปนี้

- ☐ Denial of Service & Distributed Denial of Service (DoS&DDoS)
- ☐ Session Hijacking and Man-in-the-Middle Attacks
- ☐ Phishing
- ☐ SQL Injection Attack
- ☐ Cross-Site Scripting (XSS)
- ☐ Malware
- ☐ Ransomware
- ☐ Insider Threat
- ☐ Credential Reuse
- ☐ Botnets
- ☐ อื่นๆ (โปรดระบุ) _____

☐ ไม่มี

21.2 โปรดระบุความถี่ในการทดสอบ Incident Response Plan สำหรับภัยคุกคามทางไซเบอร์

☐ 1 ครั้ง/ปี

☐ 2 ครั้ง/ปี

☐ มากกว่า 2 ครั้ง/ปี

☐ ไม่มีการทดสอบ

21.3 บริษัทมีการทดสอบแผน BCP สำหรับภัยคุกคามทางไซเบอร์ หรือไม่

☐ มี ☐ ไม่มี

21.4 บริษัทมีการจัดอบรมเรื่องแผน BCP สำหรับภัยคุกคามทางไซเบอร์ ให้กับพนักงานหรือไม่

☐ มี (โปรดระบุความถี่)

- ☐ 1 ครั้ง/ปี
- ☐ 2 ครั้ง/ปี
- ☐ มากกว่า 2 ครั้ง/ปี

☐ ไม่มีการทดสอบ

21.5 บริษัทมีการจัดการฝึกซ้อมรับมือภัยคุกคามทางไซเบอร์ (Cyber Exercise) หรือไม่ (ตอบได้มากกว่า 1 ข้อ)

☐ มี โดยจัดในรูปแบบต่อไปนี้

- ☐ Table Top Exercise
- ☐ Cyber Ranges
- ☐ อื่นๆ (โปรดระบุ) _____

☐ ไม่มี

21.6 โปรดระบุความถี่ในการจัด Cyber Exercise

☐ 1 ครั้ง/ปี

☐ 2 ครั้ง/ปี

☐ มากกว่า 2 ครั้ง/ปี

☐ ไม่มีการทดสอบ

22. บริษัทมีกระบวนการจัดเก็บข้อมูลเหตุการณ์ภัยคุกคามทางไซเบอร์ (Cyber Incident) ที่เคยเกิดขึ้นและนำมาศึกษาเพื่อพัฒนา BCM สำหรับภัยคุกคามทางไซเบอร์ และกระบวนการรับมือเหตุการณ์ความมั่นคงปลอดภัยทางไซเบอร์ที่อาจจะเกิดขึ้นในอนาคตหรือไม่ (Lesson Learn)

☐ มี ☐ ไม่มี

23. บริษัทได้มีการซื้อกรมธรรม์ประกันภัยที่ให้ความคุ้มครองจากภัยคุกคามทางไซเบอร์ (Cyber Insurance) หรือไม่

☐ มี ☐ ไม่มี

ส่วนที่ 4

ข้อเสนอแนะเกี่ยวกับแนวทางในการกำหนดนโยบาย

แผนรองรับการดำเนินธุรกิจอย่างต่อเนื่อง

24. ข้อเสนอแนะอื่นๆ (ถ้ามี) .....

.....

.....

.....

.....