แนวทางปฏิบัติสำหรับรักษาความปลอดภัยและควบคุมความเสี่ยงของระบบเทคโนโลยีสารสนเทศ (Information Technology Risk Management) และ ความเสี่ยงด้านภัยคุกคามทางไซเบอร์ (Cybersecurity)

<u>วัตถุประสงค์</u>

1. เพื่อให้บริษัทประกันภัย มีการกำกับดูแล นโยบาย กระบวนการ และเครื่องมือในการบริหารจัดการความเสี่ยงด้านระบบเทคโนโลยีสารสนเทศ (Information Technology Risk) และความเสี่ยงด้านภัยคุกคามทางไซเบอร์ (Cyber Risk) ที่สามารถระบุความเสี่ยง (identify) ป้องกัน (protect) ตรวจพบ (detect) รับมือ (respond) กู้ระบบคืนสู่สภาวะปกติ (recover) และสามารถดำเนินธุรกิจได้อย่างต่อเนื่อง เพื่อให้การบริหารความเสี่ยงและความปลอดภัยในการนำระบบ IT มาใช้ในการดำเนินธุรกิจมีความครอบคลุมและสามารถป้องกันความเสียหายได้อย่างทันท่วงที

2. สร้างความน่าเชื่อถือให้กับธุรกิจ (trust building) จากการที่บริษัทมีการบริหารจัดการความเสี่ยงด้านภัยคุกคามทางไซเบอร์ ควบคุมความเสี่ยงด้านระบบ IT และสามารถรักษาความปลอดภัยของข้อมูลได้อย่างรัดกุม

สำนักงาน คปภ. ได้ตระหนักถึงความสำคัญของความเสี่ยงด้านระบบเทคโนโลยีสารสนเทศ (IT Risk) รวมถึงความเสี่ยงด้านภัยคุกคามทางไซเบอร์ (Cyber risk) จึงได้กำหนดแนวทางการกำกับดูแลการบริหารจัดการความเสี่ยงด้าน IT (IT Risk Management) การรักษาความปลอดภัยของข้อมูลและระบบสารสนเทศ (IT security) การควบคุมความเสี่ยงของระบบ IT และเตรียมความพร้อมในการรับมือกับความเสี่ยงด้ายภัยคุกคามทางไซเบอร์ (Cybersecurity) เพื่อให้บริษัทประกันภัยสามารถนำไปใช้เป็นแนวทางในการควบคุมความเสี่ยงของตนเองและพัฒนาโครงสร้างพื้นฐานระบบ IT เตรียมความพร้อมเพื่อการขยายธุรกิจเข้าสู่การเป็น digital economy ตลอดจนใช้ในการพัฒนาการกำกับดูแลบริษัทประกันภัยของสำนักงาน คปภ. เพื่อให้ทันกับวิวัฒนาการของความเสี่ยงที่เปลี่ยนแปลงไปตามบริบทในการทำธุรกิจ รวมถึงกำหนดให้บริษัทมีการบริหารจัดการเหตุการณ์ที่อาจส่งผลกระทบต่อความปลอดภัยของระบบสารสนเทศ (Information technology security incident management) และในกรณีที่บริษัทถูกโจมตีทางไซเบอร์ (Cyber attack) ในระดับที่ส่งผลกระทบอย่างมีนัยสำคัญ บริษัทต้องรายงานต่อสำนักงาน คปภ. โดยไม่ชักช้าเมื่อเกิดเหตุการณ์ดังกล่าว และมีแผนรองรับการบริหารจัดการเหตุการณ์ที่อาจส่งผลกระทบต่อความปลอดภัยของระบบสารสนเทศ (incident response plan) ที่เกิดขึ้น เพื่อให้บริษัทสามารถดำเนินธุรกิจและให้บริการลูกค้าได้อย่างต่อเนื่อง

อย่างไรก็ตาม ระบบเทคโนโลยีสารสนเทศของบริษัทประกันภัยแต่ละแห่งยังคงมีความหลากหลายและแตกต่างกันค่อนข้างมาก ดังนั้น การมีมาตรฐานและแนวปฏิบัติเพื่อรักษาความปลอดภัยของระบบ IT และข้อมูลสารสนเทศจะช่วยให้บริษัทสามารถนำไปประยุกต์ใช้ในการกำกับดูแลและบริหารจัดการระบบเทคโนโลยีสารสนเทศ ได้อย่างเหมาะสมกับขนาดและความซับซ้อนของระบบ IT ของบริษัทเอง รวมถึงสามารถนำไปใช้ในการกำหนดมาตรการควบคุมความเสี่ยงของตนเองได้อย่างมีประสิทธิภาพ

กรอบแนวทางปฏิบัติสำหรับรักษาความปลอดภัยและควบคุมความเสี่ยงของระบบเทคโนโลยีสารสนเทศ

การกำกับดูแลที่ดีด้านเทคโนโลยีสารสนเทศ (IT Governance)

๑. นโยบายการรักษาความปลอดภัยของระบบเทคโนโลยีสารสนเทศ (IT Security Policy)

๒. นโยบายการบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศ (IT Risk Management)

แนวทางควบคุมความเสี่ยงของระบบเทคโนโลยีสารสนเทศของบริษัทประกันภัย

๑. การรักษาความถูกต้องปลอดภัยในการปฏิบัติงานที่เกี่ยวข้องกับระบบสารสนเทศ

๒. การควบคุมการเข้าถึงระบบสารสนเทศ และข้อมูล (access control) เพื่อป้องกันการถูกบุกรุกและเข้าถึงโดยไม่ได้รับอนุญาต

๓. การรักษาความปลอดภัยของข้อมูล

๔. การติดตามตรวจสอบความผิดปกติและช่องโหว่ของระบบสารสนเทศ

๕. การรักษาความพร้อมใช้งานของระบบสารสนเทศ และการบริหารจัดการเหตุการณ์ที่อาจส่งผลกระทบต่อความปลอดภัยของระบบสารสนเทศ

การกำกับดูแลที่ดีและการบริหารจัดการความเสี่ยงด้านภัยคุกคามทางไซเบอร์ (Cybersecurity Governance & Risk Management)

๑. การกำกับดูแลความเสี่ยงด้านภัยคุกคามทางไซเบอร์

๒. การบริหารจัดการความเสี่ยงด้านภัยคุกคามทางไซเบอร์

การกำกับดูแลที่ดีด้านเทคโนโลยีสารสนเทศ (IT Governance)

การกำกับดูแลด้านเทคโนโลยีสารสนเทศ มีจุดมุ่งหมายเพื่อทำให้แน่ใจว่า องค์กรสามารถบรรลุเป้าหมายที่กำหนดไว้ โดยนำเทคโนโลยีสารสนเทศมาใช้เป็นเครื่องมือในการสนับสนุน และสามารถบริหารจัดการความเสี่ยงที่อาจเกิดขึ้นจากการนำเทคโนโลยีมาใช้ได้อย่างมีประสิทธิภาพ การบริหารงานด้านเทคโนโลยีสารสนเทศที่ดีนั้นต้องมีการเชื่อมโยงระหว่างกระบวนการบริหารงานด้านเทคโนโลยีสารสนเทศ ทรัพยากรและข้อมูลที่มีประสิทธิภาพเพื่อสนับสนุนนโยบาย กลยุทธ์ เป้าหมายขององค์กรและการบริหารความเสี่ยงที่เหมาะสม รวมทั้งมีการรายงานและติดตามการดำเนินงาน เพื่อให้มั่นใจว่า เทคโนโลยีที่บริษัทนำมาใช้สามารถช่วยสนับสนุนกลยุทธ์และบรรลุวัตถุประสงค์ในเชิงธุรกิจและสร้างศักยภาพในการแข่งขันรวมทั้งเพิ่มมูลค่าให้กับองค์กร โดยบริษัทต้องพิจารณาดำเนินการอย่างน้อยดังต่อไปนี้

1. นโยบายการรักษาความปลอดภัยของระบบเทคโนโลยีสารสนเทศ (IT Security Policy)

1.1 คณะกรรมการบริษัทและผู้บริหารระดับสูง มีหน้าที่ดูแลให้มีการกำหนด**นโยบายการรักษาความปลอดภัยของระบบเทคโนโลยีสารสนเทศ**เป็นลายลักษณ์อักษร รวมทั้งทำหน้าที่ในการพิจารณาอนุมัตินโยบายดังกล่าว ทั้งนี้ บริษัทต้องทำการสื่อสารนโยบายดังกล่าวเพื่อสร้างความเข้าใจและให้สามารถปฏิบัติตามได้อย่างถูกต้อง โดยเฉพาะอย่างยิ่งระหว่างหน่วยงานด้านเทคโนโลยีสารสนเทศและหน่วยงานธุรกิจภายในบริษัท เพื่อให้มีการประสานงานและสามารถดำเนินธุรกิจได้ตามเป้าหมายที่ตั้งไว้

นโยบายการรักษาความปลอดภัยของระบบเทคโนโลยีสารสนเทศ (IT Security Policy) อย่างน้อยต้องครอบคลุมในเรื่องดังต่อไปนี้

- การรักษาความถูกต้องปลอดภัยในการปฏิบัติงานที่เกี่ยวข้องกับระบบสารสนเทศ
- การควบคุมการเข้าถึงระบบสารสนเทศ และข้อมูล
- การรักษาความปลอดภัยของข้อมูล
- การติดตามตรวจสอบความผิดปกติและช่องโหว่ของระบบสารสนเทศ
- การบริหารจัดการระบบ IT ให้มีความพร้อมในการรองรับการดำเนินธุรกิจอย่างต่อเนื่อง

1.2 บริษัทต้องจัดให้มี**การประเมินประสิทธิภาพของนโยบาย**การรักษาความปลอดภัยของระบบเทคโนโลยีสารสนเทศ อย่างน้อยปีละ 1 ครั้ง หรือเมื่อมีการเปลี่ยนแปลงที่มีผลกระทบต่อการรักษาความปลอดภัยของบริษัท ทั้งนี้ การประเมินประสิทธิภาพ บริษัทสามารถกระทำได้โดยหน่วยงานตรวจสอบภายในด้านเทคโนโลยีสารสนเทศของบริษัท (IT Audit) หรือผู้ตรวจสอบภายนอก เพื่อปรับปรุงแก้ไขข้อบกพร่องของการรักษาความปลอดภัยของระบบเทคโนโลยีสารสนเทศของบริษัท

1.3 ในกรณีที่บริษัท มีการใช้บริการด้านงานเทคโนโลยีสารสนเทศจากผู้ให้บริการจากภายนอก (Outsource) บริษัทต้องจัดให้มีนโยบายเพื่อรองรับการใช้บริการดังกล่าว ซึ่งต้องครอบคลุมถึงวิธีการคัดเลือกและพิจารณาคุณสมบัติของผู้ให้บริการ และมีข้อกำหนดเกี่ยวกับการใช้บริการเพื่อลดความเสี่ยงจากการเข้าถึงทรัพย์สินสารสนเทศอย่างไม่เหมาะสม รวมถึงข้อกำหนดเกี่ยวกับการรักษาความลับของข้อมูล และไม่เปิดเผยข้อมูลที่มีความสำคัญ

นอกจากนี้ บริษัทต้องมี**มาตรการ**เพื่อให้มั่นใจได้ว่าสามารถควบคุมการปฏิบัติงานของผู้ให้บริการจากภายนอกให้เป็นไปตามข้อตกลงที่กำหนดไว้ โดยสามารถตรวจสอบกระบวนการปฏิบัติงาน รวมทั้งมีแผนรองรับในกรณีที่เกิดเหตุการณ์ที่อาจส่งผลกระทบต่อความปลอดภัยของระบบสารสนเทศ (incident response plan)

2. นโยบายการบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศ (IT Risk Management)

ต้องสอดคล้องกับนโยบายการบริหารจัดการความเสี่ยงรวมของบริษัท (Enterprise Risk Management) และครอบคลุมในเรื่องดังต่อไปนี้

1. การกำหนดหน้าที่และความรับผิดชอบในการบริหารและจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศ
2. การระบุความเสี่ยงที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศ (IT-related risk)
3. การประเมินความเสี่ยง ที่ครอบคลุมถึงโอกาสหรือความถี่ที่จะเกิดความเสี่ยง และผลกระทบที่จะเกิดขึ้น เพื่อจัดลำดับความสำคัญในการบริหารจัดการความเสี่ยง
4. การกำหนดวิธีการหรือเครื่องมือในการบริหารและจัดการความเสี่ยงให้อยู่ในระดับที่องค์กรยอมรับได้
5. การกำหนดตัวชี้วัดระดับความเสี่ยง (IT risk indicator) รวมถึงจัดให้มีการติดตามและรายงานผลตัวชี้วัดดังกล่าวต่อผู้ที่มีหน้าที่รับผิดชอบ เพื่อให้สามารถบริหารและจัดการความเสี่ยงได้อย่างเหมาะสมและทันต่อเหตุการณ์

แนวทางควบคุมความเสี่ยงของระบบเทคโนโลยีสารสนเทศของบริษัทประกันภัย

1. การรักษาความถูกต้องปลอดภัยในการปฏิบัติงานที่เกี่ยวข้องกับระบบสารสนเทศ อย่างน้อยต้องครอบคลุมในเรื่องดังต่อไปนี้

1.1 บริษัทต้องกำหนดขั้นตอนการปฏิบัติงานที่เกี่ยวข้องกับระบบเทคโนโลยีสารสนเทศ เพื่อให้การปฏิบัติงานเป็นไปอย่างถูกต้องและปลอดภัย โดยกำหนดเป็นลายลักษณ์อักษรเพื่อให้พนักงานปฏิบัติการคอมพิวเตอร์ (computer operator) สามารถปฏิบัติงานได้อย่างถูกต้องและเป็นไปตามนโยบายการรักษาความปลอดภัยของระบบสารสนเทศ เช่น ขั้นตอนในการเปิด/ปิดระบบการประมวลผล การตรวจสอบประสิทธิภาพการทำงานของระบบ เป็นต้น

1.2 การรับ - ส่งข้อมูลสารสนเทศ (Information transfer) ทั้งภายในและภายนอกองค์กร บริษัทต้องรักษาความปลอดภัยของข้อมูลที่มีการรับส่งผ่านระบบเครือข่ายคอมพิวเตอร์ โดยมีการป้องกันการเปลี่ยนแปลงแก้ไขหรือทำความเสียหายกับข้อมูล และโปรแกรมไม่ประสงค์ดี (malware) ที่ถูกส่งผ่านช่องทางการสื่อสาร มีการป้องกันข้อมูลที่เป็นความลับหรือมีความสำคัญที่รับส่งในรูปแบบของไฟล์แนบ (attachment files) และการส่งต่อจดหมายอิเล็กทรอนิกส์แบบอัตโนมัติออกสู่ภายนอกองค์กร โดยการเข้ารหัสข้อมูลมาใช้ในการรับส่งข้อมูลสารสนเทศ

1.3 บริษัทต้องมีมาตรการป้องกันและตรวจสอบภัยคุกคามจากโปรแกรมที่ไม่ประสงค์ดี (Malware) โดยติดตั้งโปรแกรมป้องกัน Malware ให้ครอบคลุมทั้งเครื่องประมวลผลและเครื่องคอมพิวเตอร์พร้อมทั้งปรับปรุงโปรแกรมป้องกันให้เป็นปัจจุบัน และสามารถแก้ไขระบบเทคโนโลยีสารสนเทศให้สามารถกลับมาใช้งานได้ตามปกติ นอกจากนี้ บริษัทต้องมีระบบหรือกระบวนการในการป้องกันเพื่อลดความเสี่ยงจากการทำ website เลียนแบบ (Phishing)

1.4 บริษัทต้องกำหนดให้มีการสำรองข้อมูลที่สำคัญทางธุรกิจ ระบบปฏิบัติการ โปรแกรมประยุกต์ ระบบงานคอมพิวเตอร์อย่างครบถ้วน และกำหนดเป้าหมายในการกู้คืนข้อมูล (Recovery Point Objective: RPO) เช่น ประเภทของข้อมูล และชุดข้อมูลล่าสุดที่จะกู้คืนได้ โดยบริษัทต้องจัดเก็บสื่อบันทึกข้อมูลสำรองไว้นอกสถานที่เพื่อความปลอดภัยในกรณีที่สถานที่ปฏิบัติงานได้รับความเสียหาย และต้องทำการทดสอบข้อมูลสำรองและกระบวนการกู้คืนข้อมูลอย่างน้อยปีละ 1 ครั้ง ทั้งนี้ บริษัทต้องมีการป้องกันความเสียหายของข้อมูลที่ทำการสำรองไว้ด้วย

<u>การสำรองข้อมูล บริษัทต้องกำหนดวิธีปฏิบัติอย่างน้อยดังนี้</u>

- ข้อมูลที่ต้องสำรอง และความถี่ในการสำรอง
- ประเภทสื่อที่ใช้ในการบันทึกข้อมูล (media)
- จำนวนที่ต้องสำรอง (copy)
- ขั้นตอนและวิธีการสำรองข้อมูล
- สถานที่และวิธีการเก็บรักษาสื่อบันทึกข้อมูล
- กระบวนการกู้คืนข้อมูลในกรณีที่ข้อมูลสูญหาย

ทั้งนี้ สถานที่ในการจัดเก็บข้อมูลสำรอง บริษัทต้องคำนึงถึงความมั่นคงปลอดภัยและต้องมีระยะห่างจากสำนักงานใหญ่เพียงพอที่จะไม่ได้รับผลกระทบเดียวกันและต้องไม่ใช้ระบบสาธารณูปโภค (น้ำประปา ไฟฟ้า อินเตอร์เน็ต) จากแหล่งเดียวกัน รวมถึงต้องมีการควบคุมสภาพแวดล้อมของห้องเก็บสื่อบันทึกข้อมูล และป้องกันความเสียหายของสื่อ

ในกรณีที่จำเป็นต้องจัดเก็บข้อมูลเป็นระยะเวลานาน ต้องคำนึงถึงวิธีการนำข้อมูลกลับมาใช้งานในอนาคตด้วย เช่น กรณีที่จัดเก็บข้อมูลในสื่อบันทึกประเภทใด ต้องมีการเก็บอุปกรณ์และโปรแกรม ที่เกี่ยวข้องสำหรับใช้อ่านสื่อบันทึกประเภทนั้นไว้ด้วยเช่นกัน เป็นต้น

1.5 จัดเก็บและบันทึกหลักฐาน (logs) ต่างๆ ของการเข้าใช้งานระบบเทคโนโลยีสารสนเทศ ให้ครบถ้วนและเพียงพอสำหรับการตรวจสอบ โดยอย่างน้อยต้องครอบคลุมการเข้าถึงและใช้งานระบบสารสนเทศ (application log) การใช้งานแฟ้มข้อมูล และการใช้อินเทอร์เน็ตผ่านระบบเครือข่ายคอมพิวเตอร์ภายในของบริษัท (internet access log)

1.6 ควบคุมและจำกัดสิทธิการติดตั้งซอฟท์แวร์บนระบบงาน เพื่อให้ระบบปฏิบัติงานมีความถูกต้องครบถ้วนและน่าเชื่อถือ **รวมถึงทำการทดสอบการเจาะระบบ (penetration test) กับระบบงานที่มีความสำคัญ**ที่เชื่อมต่อกับระบบเครือข่ายภายนอกก่อนทำการติดตั้งบนระบบงานของบริษัท เพื่อตรวจหาช่องโหว่ที่อาจเกิดขึ้น (technical vulnerability management) ของซอฟแวร์ที่จะติดตั้งใหม่อย่างเหมาะสม ในกรณีที่มีการติดตั้ง feature เพิ่มเติมบนระบบงานเก่า บริษัทต้องพิจารณาทำการทดสอบหาก feature ใหม่มีผลกระทบต่อระบบงานที่ใช้อยู่แล้ว

1.7 การใช้บริการ Cloud Computing จากผู้ให้บริการภายนอกด้านโครงสร้างพื้นฐานเทคโนโลยีสารสนเทศและระบบงานสารสนเทศ เพื่อการจัดเก็บข้อมูล การประมวลผล หรือดำเนินการใดๆ ที่เกี่ยวข้องกับข้อมูลของบริษัท

บริษัทต้องกำหนดหลักเกณฑ์วิธีการคัดเลือกผู้ให้บริการ และมาตรฐานการให้บริการของผู้ให้บริการ Cloud Computing อย่างชัดเจน โดยต้องให้ความสำคัญในเรื่องการรักษาความปลอดภัยของข้อมูล ความถูกต้องเชื่อถือได้ของข้อมูลและระบบสารสนเทศ และความพร้อมใช้งานของระบบสารสนเทศที่ใช้บริการ รวมถึงกำหนดคุณสมบัติของผู้ให้บริการ เช่น ฐานะการเงิน ความเพียงพอของการให้บริการเพื่อให้มั่นใจได้ว่าผู้ให้บริการสามารถให้บริการตามความต้องการของบริษัทได้อย่างต่อเนื่อง ทั้งนี้ บริษัทควรมีการติดตาม ประเมิน และทบทวนการให้บริการและคุณสมบัติของผู้ให้บริการ Cloud Computing เป็นประจำอย่างน้อยทุกปี

ในการนี้ บริษัทใดมีการใช้บริการ Cloud Computing จากผู้ให้บริการภายนอกให้แจ้งต่อสำนักงาน คปภ. ก่อนการใช้บริการด้วย ทั้งนี้ หากบริษัทใดที่ใช้บริการ Cloud Computing จากผู้ให้บริการภายนอกอยู่ก่อนแล้ว บริษัทต้องรายงานต่อสำนักงาน คปภ. โดยทันทีหลังจากแนวทางปฏิบัติฉบับนี้ได้เผยแพร่ให้ทุกบริษัทนำไปปฏิบัติอย่างเป็นทางการ

2. การควบคุมการเข้าถึงระบบสารสนเทศ และข้อมูล (access control) เพื่อป้องกันการถูกบุกรุกและเข้าถึงโดยไม่ได้รับอนุญาต อย่างน้อยต้องครอบคลุมในเรื่องดังต่อไปนี้

2.1 การควบคุมการเข้าถึงระบบและข้อมูลสารสนเทศ

บริษัทต้องกำหนดสิทธิในการเข้าถึงระบบและข้อมูลให้เหมาะสมตามความจำเป็นและหน้าที่ความรับผิดชอบของผู้ใช้งาน เพื่อป้องกันการรั่วไหลของข้อมูลและแก้ไขฐานข้อมูลโดยไม่ได้รับอนุญาต โดยกำหนดให้ผู้ใช้งานต้องยืนยันตัวบุคคลโดยกำหนด Username และ Password เพื่อเข้าถึงข้อมูลได้ตามสิทธิที่กำหนด และบันทึกการเข้าถึงระบบโดยบัญชีผู้ใช้ทุกประเภท (access log)

ทั้งนี้ บริษัทต้องมีข้อกำหนดเกี่ยวกับผู้ใช้งานที่ได้รับสิทธิให้เข้าถึงระบบและข้อมูลในการดูแลการใช้สิทธิที่ได้รับ รวมถึงกรณีที่มีความจำเป็นต้องให้สิทธิบุคคลอื่นในการใช้งานระบบคอมพิวเตอร์ และมีการอนุมัติจากผู้มีอำนาจทุกครั้ง โดยบันทึกเหตุผลและความจำเป็นรวมถึงกำหนดระยะเวลาในการใช้งาน

2.2 การกำหนดมาตรการเพื่อสร้างความปลอดภัยทางกายภาพและสภาพแวดล้อมของทรัพย์สินสารสนเทศ (Physical and environment security)

บริษัทต้องจัดพื้นที่ในการจัดวางทรัพย์สินสารสนเทศที่มีความสำคัญ เช่น ห้องเซิร์ฟเวอร์ ศูนย์คอมพิวเตอร์ เป็นต้น ให้มีความปลอดภัยและป้องกันมิให้บุคคลที่ไม่เกี่ยวข้องเข้าถึงพื้นที่ดังกล่าว โดยต้องคำนึงถึงความปลอดภัยจากภัยธรรมชาติ และภัยคุกคามจากมนุษย์ และมีความมิดชิดรวมทั้งป้องกันมิให้มีการเปิดเผยข้อมูลและรายละเอียดของพื้นที่หวงห้ามต่อสาธารณะ บริษัทต้องกำหนดสิทธิการเข้าออกพื้นที่หวงห้ามให้เฉพาะบุคคลที่มีหน้าที่เกี่ยวข้อง และระบบการควบคุมการเข้าออกอย่างรัดกุม และบริษัทต้องบันทึกข้อมูลการเข้า-ออกห้องเซิร์ฟเวอร์ หรือ ศูนย์คอมพิวเตอร์ รวมถึงต้องจัดให้มีการรักษาความมั่นคงปลอดภัย เช่น มีระบบกล้องวงจรปิด เครื่องสแกนลายนิ้วมือ อุปกรณ์เตือนไฟไหม้ ถังดับเพลิงหรือระบบดับเพลิงแบบอัตโนมัติ ระบบไฟฟ้าสำรอง (uninterrupted power supply) เป็นต้น ทั้งนี้ บริษัทต้องมีมาตรการป้องกันทรัพย์สินสารสนเทศประเภทอุปกรณ์ มิให้เกิดการสูญหาย ถูกโจรกรรม ถูกเข้าถึง หรือถูกใช้งานโดยบุคคลที่ไม่เกี่ยวข้อง

3. การรักษาความปลอดภัยของข้อมูล (Data Security)

บริษัทต้องมีกระบวนการในการรักษาความปลอดภัยของข้อมูล ที่เพียงพอแก่การป้องกันไม่ให้บุคคลที่ไม่มีอำนาจเกี่ยวข้องเข้าถึง หรือสามารถเปลี่ยนแปลงแก้ไขข้อมูล หรือนำข้อมูลไปใช้ประโยชน์ ในทางที่ผิดกฎหมาย โดยเฉพาะอย่างยิ่งข้อมูลของผู้เอาประกันภัย โดยแนวทางการรักษาความปลอดภัยของข้อมูลอย่างน้อยต้องครอบคลุมในเรื่องดังต่อไปนี้

3.1 บริษัทต้องทำ**การระบุว่า <u>ข้อมูลอะไรบ้างที่เป็นข้อมูลที่สำคัญหรือเป็นข้อมูลความลับของบริษัท</u> และทำการจัดประเภทข้อมูลตามระดับชั้นความลับและความสำคัญ** เพื่อให้ข้อมูลที่สำคัญได้รับการปกป้องในระดับที่เหมาะสมตามระดับชั้นความลับ

3.2 **กำหนดสิทธิ์ในการเข้าถึงข้อมูลที่สำคัญหรือข้อมูลความลับ เพื่อป้องกันการเข้าถึงและแก้ไขเปลี่ยนแปลงข้อมูลโดยผู้ที่ไม่มีสิทธิหรือไม่ได้รับอนุญาต** ทั้งนี้ ต้องเพียงพอสำหรับใช้ในการทำงานปกติและสอดคล้องกับหน้าที่การปฏิบัติงานของเจ้าหน้าที่ที่เกี่ยวข้อง การควบคุมที่มีประสิทธิภาพจะต้องสามารถป้องกันและจำกัดการเข้าถึงตามที่สิทธิที่กำหนดไว้ได้

3.3 **การรับส่งข้อมูลสำคัญผ่านเครือข่ายสาธารณะ บริษัทต้องทำการเข้ารหัสข้อมูล (cryptographic control)** เพื่อป้องกันการเข้าถึงหรือเปลี่ยนแปลงแก้ไขข้อมูลให้สอดคล้องและเหมาะสมกับระดับความเสี่ยงที่อาจเกิดขึ้น

3.4 **การจัดเก็บข้อมูลสำคัญหรือข้อมูลที่มีชั้นความลับ** บริษัทต้องรักษาความปลอดภัยของข้อมูลโดยการเข้ารหัสข้อมูล (encryption) ที่สามารถป้องกันการนำข้อมูลสำคัญไปใช้ประโยชน์ในทางที่ผิดในกรณีข้อมูลรั่วไหล และสอดคล้องเหมาะสมกับระดับความเสี่ยงที่อาจเกิดขึ้นกับข้อมูลที่มีความสำคัญ รวมทั้งกำหนดผู้รับผิดชอบในการบริหารจัดการการเข้ารหัสข้อมูล

4. การติดตามตรวจสอบความผิดปกติและช่องโหว่ของระบบสารสนเทศ

บริษัทต้องทำการประเมินช่องโหว่ (vulnerability assessment) กับระบบงานที่มีความสำคัญทุกระบบอย่างน้อยปีละ 1 ครั้ง และเมื่อมีการเปลี่ยนแปลงระบบงานดังกล่าวอย่างมีนัยสำคัญ โดยอย่างน้อยต้องจัดให้มีกระบวนการประเมินหรือตรวจสอบหาช่องโหว่ของระบบ และมีมาตรการดำเนินการรองรับเพื่อปิดช่องโหว่ หรือกำหนดแผนรองรับกรณีที่ระบบถูกบุกรุกผ่านช่องโหว่ โดยบริษัทต้องกำหนดผู้รับผิดชอบในการจัดการเกี่ยวกับช่องโหว่ของระบบและดำเนินการปิดช่องโหว่ที่พบโดยไม่ชักช้า (patching) ทั้งนี้ ต้องมีการบันทึกและจัดเก็บหลักฐานเพื่อการตรวจสอบในการดำเนินการต่าง ๆ ที่เกี่ยวข้องกับการจัดการช่องโหว่ของระบบด้วย

5. การรักษาความพร้อมใช้งานของระบบสารสนเทศ และการบริหารจัดการเหตุการณ์ที่อาจส่งผลกระทบต่อความปลอดภัยของระบบสารสนเทศ

5.1 บริษัทต้องมีการบริหารจัดการเหตุการณ์ที่อาจส่งผลกระทบต่อความมั่นคงปลอดภัยของระบบสารสนเทศ **(information security incident management)** โดยอย่างน้อยครอบคลุมในเรื่องดังต่อไปนี้

- **กำหนดแผนรองรับในกรณีที่เกิดเหตุการณ์ที่อาจส่งผลกระทบต่อความมั่นคงปลอดภัยของระบบสารสนเทศ (Incident response plan) อย่างเป็นลายลักษณ์อักษร** และประเมินเหตุการณ์หรือจุดอ่อนของการรักษาความปลอดภัยระบบสารสนเทศ เพื่อพิจารณาระดับความรุนแรงของเหตุการณ์และผลกระทบต่อความมั่นคงปลอดภัยของระบบสารสนเทศ และต้องจัดให้มีการทดสอบกระบวนการในการบริหารจัดการเหตุการณ์ที่อาจส่งผลกระทบต่อความมั่นคงปลอดภัยของระบบสารสนเทศอย่างน้อยปีละ 1 ครั้ง

ทั้งนี้ บริษัทต้องจัดให้มีบุคคลหรือหน่วยงานเพื่อทำหน้าที่รับแจ้งเหตุการณ์ที่เกิดขึ้น และทำหน้าที่ในการรายงานเหตุการณ์ต่อผู้บริหารระดับสูงหรือผู้เกี่ยวข้องให้ทราบและดำเนินการต่อไป

- **จัดให้มีบุคคลหรือหน่วยงาน (point of contact)** เพื่อทำหน้าที่**รายงานเหตุการณ์ที่เกิดขึ้นต่อสำนักงาน คปภ.** โดยให้รายงานดังต่อไปนี้

รายงานทันทีเมื่อเกิดเหตุ	**ระหว่างดำเนินการแก้ไข**	**แก้ไขปัญหาได้ และเหตุยุติ**
1. วันเวลาที่เกิดเหตุการณ์ 2. หน่วยงาน / ระบบที่เกิดเหตุ รายละเอียดและสาเหตุของเหตุการณ์ที่เกิดขึ้น 3. ผลกระทบที่คาดว่าจะเกิดขึ้น 4. ชื่อผู้ติดต่อ / ประสานงานของบริษัทเพื่อให้ข้อมูล	1. วันเวลาที่เกิดเหตุการณ์ 2. หน่วยงาน / ระบบที่เกิดเหตุ รายละเอียดและสาเหตุของเหตุการณ์ที่เกิดขึ้น 3. ผลกระทบที่คาดว่าจะเกิดขึ้นโดยประเมินมูลค่าความเสียหายที่อาจเกิดขึ้นกับผู้เอาประกันภัยและบริษัท 4. การดำเนินการแก้ไขปัญหา และระยะเวลาในการแก้ไข 5. ความคืบหน้าในการแก้ไขปัญหา	1. วันเวลาที่เกิดเหตุการณ์ 2. หน่วยงาน / ระบบที่เกิดเหตุ รายละเอียดและสาเหตุของเหตุการณ์ที่เกิดขึ้น 3. ผลกระทบที่คาดว่าจะเกิดขึ้นโดยประเมินมูลค่าความเสียหายที่อาจเกิดขึ้น กับผู้เอาประกันภัยและบริษัท 4. การดำเนินการแก้ไขปัญหา 5. ผลการแก้ไขปัญหา และระยะเวลาในการแก้ไข 6. แนวทางป้องกันในอนาคต และการเก็บรวบรวมหลักฐานเพื่อระบุสาเหตุและแนวทางแก้ไขต่อไป
รายงานโดยไม่ชักช้าเมื่อทราบเหตุการณ์และตรวจสอบยืนยันในเบื้องต้นแล้ว	รายงานภายใน 2 วันทำการถัดไปหลังทราบเหตุการณ์และตรวจสอบยืนยันแล้ว	รายงานเมื่อเหตุการณ์ยุติหรือแก้ไขปัญหาแล้วเสร็จภายใน 15 วัน

5.2 บริษัทต้องกำหนดให้มีการบริหารความต่อเนื่องทางธุรกิจในด้านระบบ**สารสนเทศ (information security of business continuity management)**

5.2.1 บริษัทต้องกำหนดแผนการบริหารความต่อเนื่องทางธุรกิจด้านเทคโนโลยีสารสนเทศ (IT continuity plan) เพื่อให้บริษัทสามารถกู้ระบบสารสนเทศหรือจัดหาระบบปฏิบัติการมาดำเนินการทดแทนได้โดยเร็วเพื่อให้เกิดความเสียหาย น้อยที่สุด และยังคงดำเนินธุรกิจได้อย่างต่อเนื่อง โดยมีรายละเอียดอย่างน้อยดังนี้

- จัดลำดับความสำคัญในการกู้คืนระบบงานให้สอดคล้องกับผลกระทบที่อาจเกิดขึ้น รวมถึงความสัมพันธ์ของแต่ละระบบงาน และการกำหนดระยะเวลาในการกลับคืนสภาพการดำเนินงานตามปกติของระบบงาน
- ขั้นตอนการแก้ไขปัญหาหรือตอบสนองต่อเหตุการณ์ในแต่ละสถานการณ์ที่เกิดขึ้น
- บุคคลที่ทำหน้าที่รับผิดชอบและมีอำนาจตัดสินใจ รวมถึงกำหนดเจ้าหน้าที่ผู้รับผิดชอบที่สามารถปฏิบัติงานได้ในแต่ละสถานการณ์ รวมทั้งมีรายชื่อและเบอร์โทรศัพท์ของบุคคลที่เกี่ยวข้องทั้งหมด
- ระบุทรัพยากรที่จำเป็นสำหรับระบบงานที่สำคัญที่จำเป็นต้องใช้ เช่น ข้อมูลรายละเอียดของศูนย์คอมพิวเตอร์สำรอง สถานที่ตั้ง แผนที่ เครื่องรุ่นคอมพิวเตอร์ ระบบที่ใช้ในการปฏิบัติงาน (Systems) ข้อมูลและบันทึกต่างๆ (Records & Data) โดยบริษัทต้องมีระบบสารสนเทศที่อยู่ในสภาพพร้อมใช้งาน

5.2.2 บริษัทต้องมีการสื่อสารแผน IT continuity plan ให้แก่เจ้าหน้าที่ที่เกี่ยวข้องเพื่อรับทราบและสร้างความเข้าใจที่ตรงกัน เพื่อให้สามารถนำไปปฏิบัติได้อย่างถูกต้องเมื่อเกิดเหตุการณ์

5.2.3 ทำการทดสอบการปฏิบัติตามแผน IT continuity plan อย่างน้อยปีละ 1 ครั้ง โดยต้องกำหนดให้มีการทดสอบในลักษณะสถานการณ์ที่สอดคล้องกับลักษณะ ขอบเขต และความซับซ้อนในการดำเนินธุรกิจของบริษัท และเป็นสถานการณ์ที่มีความเป็นไปได้และสอดคล้องกับสถานการณ์ในปัจจุบันของบริษัท

การกำกับดูแลที่ดีและการบริหารจัดการความเสี่ยงด้านภัยคุกคามทางไซเบอร์
(Cybersecurity Governance & Risk Management)

ในปัจจุบันบริษัทประกันภัยจำเป็นต้องตระหนักถึงการบริหารจัดการความเสี่ยงด้านความมั่นคงปลอดภัยของภัยคุกคามทางไซเบอร์ ซึ่งการบริหารจัดการความเสี่ยงด้านระบบเทคโนโลยีสารสนเทศ (Information Technology Risk) เพียงอย่างเดียวอาจจะยังไม่เพียงพอในการรับมือกับภัยคุกคามที่ไม่อาจคาดคิด ไม่แน่นอน ไม่สามารถคาดการณ์ได้ และที่ไม่รู้ (unknown, unpredictable, uncertain, unexpected) ดังนั้น เพื่อให้บริษัทประกันภัยตระหนักและให้ความสำคัญต่อ cyber risk ที่จะเกิดขึ้น สำนักงาน คปภ. จึงได้กำหนดแนวทางปฏิบัติในเบื้องต้นที่บริษัทสามารถนำไปปรับใช้เพื่อให้การบริหารจัดการความเสี่ยงมีความครอบคลุมถึงความเสี่ยงด้านภัยคุกคามทางไซเบอร์มากขึ้น

โดยมีรายละเอียดดังนี้

1. การกำกับดูแลความเสี่ยงด้านภัยคุกคามทางไซเบอร์ (Cybersecurity Governance)

1.1 บริษัทต้อง**กำหนดบทบาทหน้าที่ความรับผิดชอบของคณะกรรมการและผู้บริหารระดับสูงในการกำกับดูแลความเสี่ยงด้านภัยคุกคามทางไซเบอร์** เพื่อให้บริษัทมีมาตรฐานในการรักษาความปลอดภัยที่สามารถระบุ (identify) ป้องกัน (protect) ตรวจพบ (detect) รับมือ (response) และสามารถกู้คืน (recovery) เพื่อกลับสู่สภาวะปกติได้ และสนับสนุนให้บริษัทมีขีดความสามารถที่เพียงพอเหมาะสมกับปริมาณและความซับซ้อนของระบบ IT ของบริษัท โดย**กำหนดนโยบายการบริหารจัดการความเสี่ยงครอบคลุมความเสี่ยงด้านภัยคุกคามทางไซเบอร์** (Cyber Risk) รวมถึงกำหนดให้มีการ**รายงานข้อมูลความเสี่ยงด้านภัยคุกคามทางไซเบอร์ให้คณะกรรมการและผู้บริหารระดับสูง** ที่ได้รับมอบหมายรับทราบเป็นประจำ

1.2 **กำหนดให้มีหน่วยงานหรือทีมงานที่ทำหน้าที่รับผิดชอบในการประเมิน ติดตามดูแล ป้องกัน และรับมือกับภัยคุกคามทางไซเบอร์ และรายงานข้อมูลความเสี่ยงด้านภัยคุกคามทางไซเบอร์ให้คณะกรรมการและผู้บริหารระดับสูง**ที่ได้รับมอบหมายรับทราบอย่างสม่ำเสมอ ทั้งนี้ บริษัทอาจพิจารณากำหนดให้มีเจ้าหน้าที่ หรือทีมงานเฉพาะที่ทำหน้าที่รับผิดชอบในการรับมือและจัดการกับเหตุการณ์ผิดปกติทางไซเบอร์ได้ทันเวลาเพื่อลดผลกระทบที่จะเกิดขึ้น

1.3 บริษัทต้อง**จัดอบรมให้ความรู้เรื่องภัยคุกคามทางไซเบอร์ (Cybersecurity Awareness)** ที่อาจเกิดขึ้นเพื่อให้พนักงานมีความรู้ความเข้าใจและตระหนักถึงความจำเป็นในการรักษาความปลอดภัยและเข้าใจถึงผลกระทบที่จะเกิดขึ้นตามมาหากเกิดเหตุการณ์ขึ้น รวมทั้งสื่อสารแนวทางการป้องกันและการรับมือต่อเหตุการณ์ภัยคุกคามทาง ไซเบอร์

1.4 **กำหนดให้มีช่องทางในการประสานงานระหว่างหน่วยงานภายในและภายนอกองค์กรอย่างชัดเจน** รวมถึงผู้ให้บริการจากภายนอก เพื่อกำหนดแนวทางในการรับมือและแก้ไขเหตุการณ์ทางด้านความปลอดภัยได้อย่างมีประสิทธิภาพและทันเวลา

2. การบริหารจัดการความเสี่ยงด้านภัยคุกคามทางไซเบอร์

2.1 บริษัทต้องกำหนด**นโยบายในการรักษาความปลอดภัยของระบบเทคโนโลยีสารสนเทศ ที่ครอบคลุมการระบุความเสี่ยงด้านภัยคุกคามทางไซเบอร์ การป้องกัน การตรวจพบ การรับมือและการกู้คืน** รวมทั้งทบทวนและอัพเดทข้อมูลภัยคุกคามทางไซเบอร์ใหม่ๆ ตลอดเวลา เพื่อให้เท่าทันต่อการเปลี่ยนแปลงที่เกิดขึ้น

โดยมีรายละเอียดดังนี้

2.1.1 การระบุ (Identify)

บริษัทต้องทำการระบุว่า กระบวนการดำเนินงานและทรัพย์สินสารสนเทศใดบ้างที่มีความเสี่ยงต่อการถูกโจมตีทางไซเบอร์ และต้องได้รับการรักษาความมั่นคงปลอดภัย เพื่อบริหารจัดการความเสี่ยงด้านภัยคุกคามทางไซเบอร์ที่มีต่อระบบ ทรัพย์สิน ข้อมูล ของบริษัทได้อย่างเหมาะสม

2.1.2 การป้องกัน (Protect)

บริษัทต้องมีมาตรการป้องกันที่เหมาะสมเพื่อจำกัดผลกระทบของเหตุการณ์ภัยคุกคามไซเบอร์ ซึ่งครอบคลุมถึงเรื่องการควบคุมการเข้าถึง การฝึกอบรมและการสร้างความตระหนักให้แก่พนักงานและผู้ที่เกี่ยวข้อง ความปลอดภัยของข้อมูล และมาตรการด้านความมั่นคงปลอดภัยต่าง ๆ ทั้งกระบวนการและวิธีปฏิบัติ ตลอดจนเทคโนโลยี นอกจากนี้ บริษัทต้องทำการบำรุงรักษาอุปกรณ์และซอฟต์แวร์ที่เกี่ยวข้องกับระบบอิเล็กทรอนิกส์อย่างสม่ำเสมอเพื่อให้สามารถรองรับการดำเนินงานได้อย่างต่อเนื่อง รวมทั้งการเปลี่ยนแปลงแก้ไข Patch หรือ update software

2.1.3 การตรวจจับ (Detect)

บริษัทต้องมีกระบวนการติดตามเฝ้าระวัง และตรวจจับเหตุการณ์ภัยคุกคามทางไซเบอร์อย่างต่อเนื่อง และแจ้งเตือนถึงสิ่งที่ผิดปกติต่างๆ รวมถึงการติดตามเหตุการณ์ภัยคุกคามทางไซเบอร์ที่เกิดขึ้นจากทั้งภายในและภายนอก วิเคราะห์จุดอ่อนหรือช่องโหว่ของภัยคุกคามที่เกิดขึ้น เพื่อเป็นข้อมูลประกอบในการพิจารณาทบทวนแนวทางการป้องกันความเสี่ยงและผลกระทบที่จะเกิดขึ้นกับบริษัทในอนาคต

2.1.4 การตอบสนอง / การรับมือ (Respond)

บริษัทต้องกำหนดแผนการรับมือกับเหตุการณ์ภัยคุกคามทางไซเบอร์และแนวทางแก้ไขปัญหา รวมถึงจัดทำแผนการดำเนินธุรกิจอย่างต่อเนื่องให้ครอบคลุมกรณีที่ผลกระทบหรือความเสียหายจากภัยคุกคามทางไซเบอร์ทำให้การดำเนินงานหยุดชะงัก เพื่อให้สามารถรักษาระดับความปลอดภัยและการให้บริการอย่างต่อเนื่อง และบริษัทต้องทำการวิเคราะห์หาสาเหตุและตรวจหาหลักฐานของภัยคุกคามที่เกิดขึ้น รวมถึงมีกระบวนการสื่อสารกับลูกค้า ประชาชน และผู้มีส่วนได้เสียที่ชัดเจน เพื่อความเข้าใจที่ถูกต้องตรงกันต่อสถานการณ์ที่เกิดขึ้นของบริษัท

2.1.5 การกู้คืน (Recovery)

บริษัทต้องกำหนดแผนและกระบวนการในการกู้คืนระบบให้สามารถกลับมาดำเนินการได้ตามปกติภายในระยะเวลาที่กำหนด รวมถึงทำการทบทวนปรับปรุงแผนให้เป็นปัจจุบันเพื่อให้ทันต่อสถานการณ์และนำบทเรียนที่ได้รับจากเหตุการณ์ภัยคุกคามที่เกิดขึ้น (Lesson Learned) มาเป็นส่วนหนึ่งในการทบทวนแผนและกระบวนการกู้คืนระบบให้มีประสิทธิภาพยิ่งขึ้นเพื่อป้องกันปัญหาและผลกระทบที่จะเกิดขึ้นซ้ำในอนาคต