นโยบายเกี่ยวกับคู่มือระบบบริหารความมั่นคงปลอดภัยระบบสารสนเทศ

ISMS Manual

รุ่นเอกสาร	1.5	เลขที่เอกสาร	ISMS-PL-09
สายงาน	บริหารความมั่นคงปลอดภัยระบบสารสนเทศ		
กลุ่ม	ดิจิทัลทรานส์ฟอร์เมชั่น		
อนุมัติโดย			
นโยบายนี้ให้มีผลใช้บังคับ ตั้งแต่วันที่ 22 สิงหาคม 2566 เป็นต้นไป ตามมติที่ประชุมคณะทำงานกำกับดูแลการปฏิบัติงานด้านเทคโนโลยีสารสนเทศ ครั้งที่ 3 เมื่อวันที่ 22 สิงหาคม 2566 ลงนามโดย  คุณเคียน ฮิน ลิม (President)			

ประวัติการแก้ไข

รุ่นเอกสาร	วันที่	รายละเอียด	ทบทวนโดย
1.0	30/06/2017	จัดทำเอกสาร	นายมานะ ขจรมาศบุษป์
1.1	22/03/2019	ปรับปรุงเอกสาร	นายมานะ ขจรมาศบุษป์ นางกรกมล สุภวัฒนากูล
1.2	30/04/2020	ปรับปรุงเอกสาร	นายเต็มภาคย์ ภัทรรัชต์ภาคย์
1.3	04/06/2021	ปรับปรุงเอกสาร	นายเต็มภาคย์ ภัทรรัชต์ภาคย์
1.4	27/07/2022	ทบทวนเอกสาร	นายสุวัฒชัย สันตินรศักดิ์
1.5	16/05/2023	ปรับปรุงเอกสาร - ปรับปรุงบริบทภายนอก - ข้อ 5.9 และเอกสารอ้างอิงยกเลิก คส.1-10/2558 นโยบายด้านเทคโนโลยีสารสนเทศ - ยกเลิกเอกสารอ้างอิง รบ.1-6/2558 ข้อบังคับในการใช้งานระบบสารสเทศ - เพิ่มเติมเอกสารอ้างอิง รบ.1-2/2565 ระเบียบข้อบังคับเพื่อความปลอดภัยในการใช้งานระบบสารสนเทศ	น.ส.เมกรินทร์ วุฒิทา

นโยบายเกี่ยวกับคู่มือระบบบริหารความมั่นคงปลอดภัยระบบสารสนเทศ

1. บทนำ

1.1. วัตถุประสงค์ของระบบ ISMS

- เพื่อปกป้องข้อมูลและระบบสารสนเทศให้มีความมั่นคงปลอดภัย และสร้างความเชื่อมั่นให้แก่ผู้ที่เกี่ยวข้อง
- เพื่อสร้างกระบวนการที่มีประสิทธิภาพในการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศภายในบริษัทฯ และเป็นรากฐานที่สำคัญในการกำกับดูแลกิจการที่ดี
- เพื่อสนับสนุนการเติบโตของธุรกิจและการดำเนินงานของบริษัทฯ
- เพื่อวางรากฐานในการสร้างความสอดคล้องกับกฎหมายและข้อกำหนดที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยสารสนเทศ

1.2. ขอบเขต

ครอบคลุมถึงระบบบริหารจัดการความมั่นคงปลอดภัยด้านสารสนเทศของ Data Center ของบริษัทฯ

1.3. คำจำกัดความ

- **บริษัทฯ** หมายถึง บริษัท ไทยประกันชีวิต จำกัด (มหาชน) (Thai Life Insurance Public Company Limited)
- **MR (Management Representative)** หมายถึง ตัวแทนฝ่ายบริหารระบบมาตรฐาน ในที่นี้ได้แก่ ISMR หรือ ISMA
- ระบบ **ISMS (Information Security Management System)** หมายถึง ระบบการบริหารจัดการความมั่นคงปลอดภัยด้านสารสนเทศของบริษัทฯ
- **บริบทภายใน (Internal Context)** หมายถึง ปัจจัยภายในที่เป็นเหตุผลในการพิจารณาขอบข่ายของระบบ ISMS
- **บริบทภายนอก (External Context)** หมายถึง ปัจจัยภายนอกที่เป็นเหตุผลในการพิจารณาขอบข่ายของระบบ ISMS

2. บริบทขององค์กร (Context of an organization)

บริษัทฯ ได้กำหนดบริบทขององค์กรที่ครอบคลุมถึง บริบทภายใน (Internal context), บริบทภายนอก (External context) และความต้องการและความคาดหวังของผู้ที่เกี่ยวข้อง (Needs and expectations of interested parties) ไว้ดังนี้

2.1. บริบทภายใน (Internal context)

- ต้องการให้มีการกำกับดูแลตามนโยบายของบริษัทฯ
- เพื่อให้มีความสอดคล้องกับการดำเนินกลยุทธ์ของบริษัทฯ เพื่อทำให้บริษัทฯ มีความน่าเชื่อถือ มีประสิทธิภาพ ประสิทธิผลในการดำเนินงาน ตอบสนองความต้องการและความคาดหวังของผู้บริหารและผู้ที่มีส่วนได้เสีย
- ต้องการจัดการทรัพยากรที่มีอยู่ในบริษัทฯ ได้อย่างมีประสิทธิภาพ
- ต้องการสร้างกระบวนการที่มีประสิทธิภาพในการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศของบริษัทฯ และวางรากฐานการประยุกต์ใช้กระบวนการบริหารความมั่นคงปลอดภัยสารสนเทศในส่วนงานอื่นๆ ของบริษัทฯ
- เพื่อให้มีระบบการจัดการความมั่นคงปลอดภัยสารสนเทศของบริษัทฯ ตามมาตรฐานสากล (ISO/IEC 27001)

2.2. บริบทภายนอก (External context)

- ต้องการปกป้องภัยคุกคาม และความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศ
- ต้องปฏิบัติตามประกาศสำนักงานคณะกรรมการกำกับและส่งเสริมการประกอบธุรกิจประกันภัย
- ต้องปฏิบัติตามกฎหมาย และประกาศจากหน่วยงานกำกับดูแลที่เกี่ยวข้อง
- เพื่อสร้างความเชื่อมั่นให้แก่ ลูกค้า และผู้ใช้งานของบริษัทฯ ว่าระบบสารสนเทศมีความมั่นคงปลอดภัย
- เพื่อเตรียมความพร้อมต่อภาวะฉุกเฉินและการเกิดอุบัติการณ์ต่างๆ เพื่อลดความเสียหายและทำให้บริษัทฯ สามารถดำเนินงานได้อย่างต่อเนื่อง เช่น ระบบสารสนเทศล่ม การโจมตีผ่านทางไซเบอร์ (cyber-attack) เป็นต้น

2.3. ความต้องการและความคาดหวังของผู้ที่เกี่ยวข้อง (Needs and expectations of interested parties)

- ความคาดหวังของผู้บริหาร คือ ต้องการให้มีการกำกับดูแลกิจการที่ดี มีการดำเนินการที่มีประสิทธิภาพ ประสิทธิผล มีความน่าเชื่อถือ สนับสนุนการเติบโตของบริษัทฯ และสร้างความเชื่อมั่นให้กับลูกค้า และผู้ใช้งาน
- ความคาดหวังของลูกค้า และผู้ใช้งาน คือ ต้องการให้ข้อมูลของลูกค้า และผู้ใช้งานมีความมั่นคงปลอดภัย ไม่ถูกเปิดเผย ไม่ถูกใช้งาน และ / หรือ ถูกเปลี่ยนแปลงโดยไม่ได้รับอนุญาต
- ความต้องการปฏิบัติตามกฎหมาย ข้อบังคับ และข้อสัญญาที่เกี่ยวข้อง เช่น พ.ร.บ. ว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ ฉบับที่ 2 พ.ศ.2560 เป็นต้น

3. ขอบข่ายของระบบ ISMS

ขอบข่ายของระบบ ISMS คือ

“The Information Security Management System applies to Data Center including Support Infrastructure, Network and Facilities operated by Thai Life Insurance Public Company Limited. This is in accordance with the Statement of Applicability (SOA)”

ที่ตั้ง

Thai Life Insurance Public Company Limited.

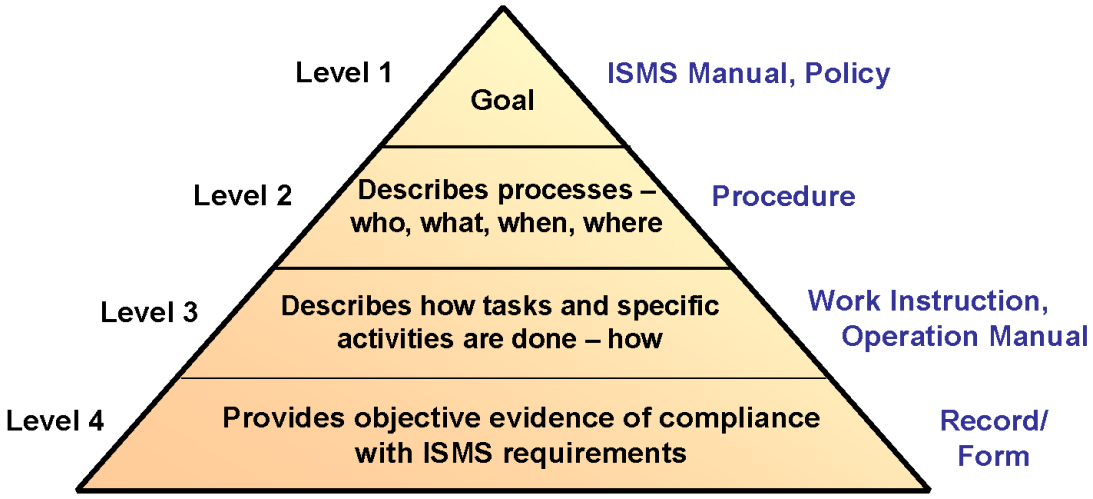
123 Ratchadaphisek Road, Dindaeng District, Bangkok 10400 Thailand

ข้อมูลโดยละเอียดเกี่ยวกับสินทรัพย์ภายใต้ขอบเขต ISMS ของ บริษัท ไทยประกันชีวิต จำกัด (มหาชน) สามารถดูได้ที่ *ISMS-FM-40 Inventory of Assets Data Center*

4. เอกสารของระบบ ISMS

4.1. ประเภทเอกสาร

เอกสารระบบ ISMS ของบริษัทฯ แบ่งเป็น 4 ประเภทดังนี้



4.2. การควบคุมเอกสาร

เอกสารระบบ ISMS ต้องได้รับการปกป้องและควบคุมอย่างเหมาะสม ดังนี้

- เอกสารต้องได้รับการอนุมัติอย่างเหมาะสมก่อนประกาศใช้งาน
- เอกสารต้องได้รับการทบทวนและปรับปรุงให้ทันสมัย และมีกระบวนการในการอนุมัติเอกสารใหม่ทุกครั้งที่มีการแก้ไขเปลี่ยนแปลงเอกสาร
- การเปลี่ยนแปลงต่อเอกสาร และ เวอร์ชั่นล่าสุดของเอกสาร ต้องได้รับการเขียนระบุอย่างเหมาะสม
- เอกสารเวอร์ชั่นล่าสุดต้องสามารถเข้าใช้งานได้โดยผู้ใช้งานที่เกี่ยวข้อง เมื่อมีความจำเป็นต้องใช้งาน
- เอกสารต้องได้รับการป้องกันการเข้าถึงและใช้งานโดยผู้ที่ไม่เกี่ยวข้องหรือไม่มีสิทธิในการใช้งาน
- เอกสารต้องมีความครบถ้วนสมบูรณ์ และอยู่ในสภาพที่พร้อมใช้งาน
- เอกสารต้องได้รับการจัดเก็บ ส่งผ่าน ใช้งาน และทำลาย ตามลำดับชั้นความลับของเอกสาร
- เอกสารจากแหล่งภายนอก ที่มีการนำมาใช้งานในบริษัท ต้องได้รับการขึ้นทะเบียนและควบคุมอย่างเหมาะสม
- เอกสารเวอร์ชั่นเก่าที่ล้าสมัย ต้องได้รับการควบคุมและจัดเก็บ เพื่อป้องกันการนำไปใช้โดยมิได้ตั้งใจ และในกรณีที่จำเป็นต้องใช้งาน เอกสารต้องได้รับการเขียนระบุอย่างชัดเจน
- อ้างอิง ISMS-PC-08 Document Control Procedure

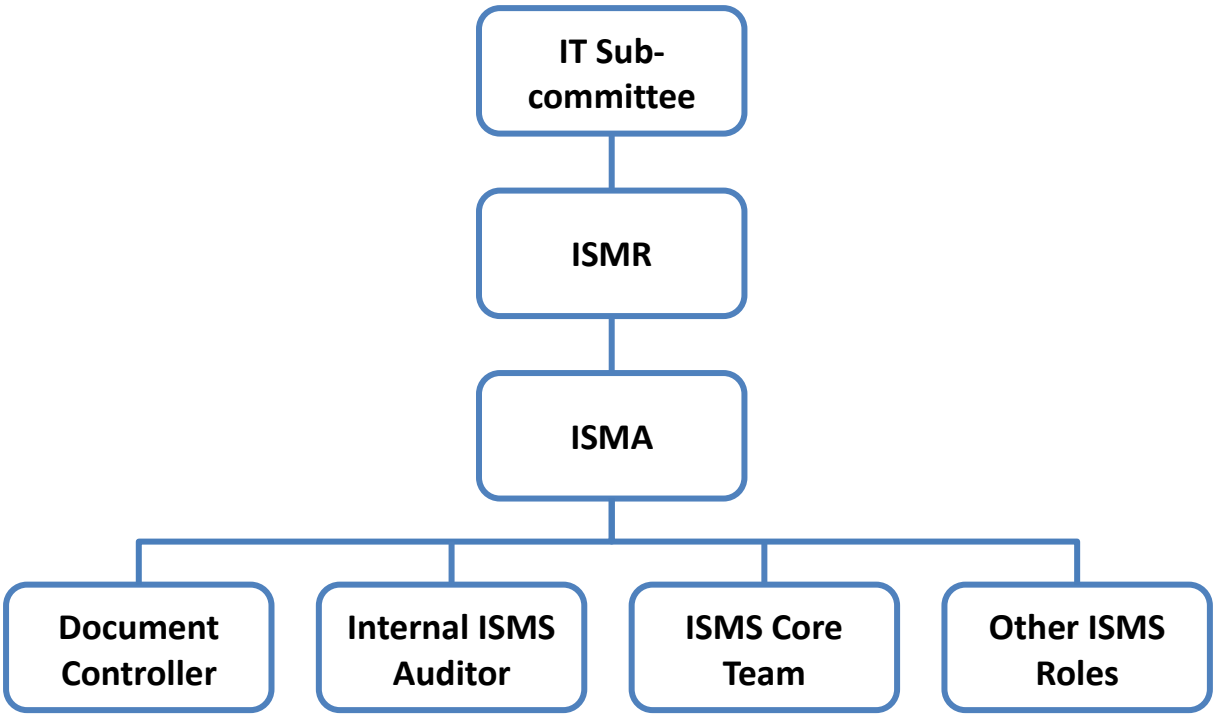
4.3. การควบคุมบันทึก

บันทึกของระบบ ISMS ถือเป็นหลักฐานของการดำเนินงานตามระบบ ISMS ซึ่งต้องได้รับการปกป้องและควบคุมอย่างเหมาะสม เพื่อให้บันทึกอยู่ในสภาพที่ครบถ้วนสมบูรณ์ สามารถนำกลับมาตรวจสอบ

ได้ และมีการปฏิบัติที่สอดคล้องตามกฎหมายหรือกฎระเบียบข้อบังคับที่เกี่ยวข้อง โดยการจัดเก็บ ใช้งาน และทำลายบันทึกต้องปฏิบัติตาม ISMS-PC-09 Record Control Procedure

- เอกสารต้องได้รับการอนุมัติอย่างเหมาะสมก่อนประกาศใช้งาน

5. โครงสร้างและหน้าที่ความรับผิดชอบในระบบ ISMS



5.1. IT Sub-committee (ITSC)

IT Sub-committee ประกอบด้วย ผู้บริหารระดับสูงจากส่วนงานที่เกี่ยวข้องที่ให้ความสนับสนุนในการจัดตั้ง ใช้งาน ตรวจสอบ และปรับปรุงระบบ ISMS ของบริษัทฯ IT Sub-committee มีหน้าที่ความรับผิดชอบดังนี้

- กำหนดวัตถุประสงค์ด้านความมั่นคงปลอดภัยสารสนเทศของบริษัทฯ
- อนุมัติและประกาศใช้งานนโยบายการรักษาความมั่นคงปลอดภัยสารสนเทศ และเอกสารต่างๆ ที่เกี่ยวข้องในระบบ ISMS
- สื่อสารให้พนักงานทุกคนตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัยของข้อมูล และการปฏิบัติตามนโยบายการรักษาความมั่นคงปลอดภัยสารสนเทศ และเอกสารต่างๆ ในระบบ ISMS

- ให้ความสนับสนุนในการให้ความรู้แก่พนักงานและบุคคลภายนอกที่เกี่ยวข้อง ให้รับทราบและสามารถปฏิบัติตามนโยบายการรักษาความมั่นคงปลอดภัยสารสนเทศ และเอกสารต่างๆ ที่เกี่ยวข้องในระบบ ISMS รวมถึงตรวจสอบการปฏิบัติตามของพนักงานและบุคคลภายนอกที่เกี่ยวข้องอย่างเหมาะสม
- พิจารณาลงโทษผู้ที่ละเมิดนโยบายการรักษาความมั่นคงปลอดภัยสารสนเทศ และเอกสารต่างๆ ที่เกี่ยวข้องในระบบ ISMS
- กำหนดเกณฑ์ในการยอมรับความเสี่ยง และระดับความเสี่ยงที่ยอมรับได้ รวมถึงพิจารณาผลการประเมินความเสี่ยงและแผนการแก้ไขความเสี่ยงที่สำคัญของบริษัทฯ
- ให้การสนับสนุนด้านทรัพยากรที่จำเป็นในการจัดตั้ง ใช้งาน ตรวจสอบ และปรับปรุงระบบ ISMS
- จัดประชุมเพื่อทบทวนการดำเนินงานของระบบ ISMS เพื่อให้มั่นใจว่าระบบ ISMS ของบริษัทฯ มีความเหมาะสม เพียงพอ และมีประสิทธิผล รวมถึงพิจารณาโอกาสในการปรับปรุงระบบ ISMS ให้ดีขึ้นอย่างต่อเนื่อง

5.2. Information Security Management Representative (ISMR) / Information Security Management Assistance (ISMA)

ISMR และ ISMA คือ ตัวแทนของผู้บริหารของบริษัทฯ ที่ทำหน้าที่ควบคุมดูแลการจัดตั้ง ใช้งาน ตรวจสอบ และปรับปรุงระบบ ISMS ของบริษัทฯ ISMR และ ISMA มีหน้าที่ความรับผิดชอบดังนี้

- ประสานงานเพื่อจัดตั้งและพัฒนาระบบ ISMS ขึ้นในบริษัทฯ รวมถึงดูแลรักษา ตรวจสอบ และปรับปรุงระบบให้มีความมั่นคงปลอดภยขึ้นอย่างต่อเนื่อง เพื่อให้บรรลุตามนโยบายการรักษาความมั่นคงปลอดภัยสารสนเทศ และสอดคล้องตามมาตรฐาน ISO/IEC 27001
- ดูแลการปรับปรุงแก้ไขนโยบาย และเอกสารต่างๆ ที่เกี่ยวข้องในระบบ ISMS ให้เหมาะสมกับการเปลี่ยนแปลงที่เกิดขึ้น สอดคล้องกับมาตรฐาน ISO/IEC 27001 และคำแนะนำที่ได้รับจาก IT Sub-committee
- สื่อสารให้พนักงานทุกคนรับทราบถึงหน้าที่และความรับผิดชอบของตนในการปฏิบัติตามนโยบายและเอกสารต่างๆ ที่เกี่ยวข้องของระบบ ISMS
- สอดส่องดูแลการปฏิบัติงานของบริษัทฯ ให้เป็นไปตามที่กำหนดไว้ในเอกสารต่างๆ ของระบบ ISMS
- ให้คำปรึกษาและแนะนำด้านการรักษาความมั่นคงปลอดภัยสารสนเทศและการนำนโยบายต่างๆ ไปใช้งาน แก่บุคลากรภายในบริษัทฯ

- ควบคุมดูแลให้มีการดำเนินกิจกรรมของระบบ ISMS ตามแผนที่วางไว้ และผลลัพธ์ที่ได้มีความสอดคล้องกับวัตถุประสงค์ด้านความมั่นคงปลอดภัยสารสนเทศของบริษัทฯ
- ควบคุมดูแลการเปลี่ยนแปลง (Change) ต่างๆ ที่เกิดขึ้นในบริษัทฯ พร้อมทั้งประสานงานให้มีการประเมิน แก้ไขและควบคุมความเสี่ยงจากการเปลี่ยนแปลงอย่างเหมาะสม
- ควบคุมดูแลการวัดประสิทธิผลของกระบวนการและ Controls ในระบบ ISMS
- ควบคุมดูแลการตรวจประเมินภายในของระบบ ISMS (Internal ISMS Audit) ให้เป็นไปอย่างเหมาะสม
- ควบคุมดูแลการดำเนินการแก้ไขและป้องกันข้อบกพร่องในระบบ ISMS รวมถึงติดตามและทบทวนประสิทธิภาพของการแก้ไขและป้องกันข้อบกพร่องอย่างเหมาะสม
- ประสานงานเพื่อจัดให้มีการประชุมเพื่อทบทวนการดำเนินงานของระบบ ISMS โดยผู้บริหาร (Management Review) และติดตามการดำเนินการตามมติที่ประชุม
- รายงานผลการดำเนินงานของระบบ ISMS ต่อผู้บริหาร
- ประสานงานและหาแนวทางในการควบคุมและจัดการปัญหา ในกรณีที่เกิดเหตุละเมิดความมั่นคง (Incident) ขึ้นในบริษัทฯ

5.3. ISMS Core Team (CT)

ISMS Core Team ประกอบด้วย ตัวแทนจากส่วนงานต่างๆ ที่อยู่ในขอบข่ายของระบบ ISMS ที่ทำหน้าที่ในการประสานงานและดำเนินงานเกี่ยวกับระบบ ISMS ของแต่ละส่วนงาน ISMS Core Team มีหน้าที่ความรับผิดชอบดังนี้

- สื่อสาร ให้คำแนะนำ และสอดส่องดูแลพนักงานในแต่ละส่วนงาน เพื่อให้สามารถปฏิบัติงานได้อย่างถูกต้องตามนโยบาย และเอกสารต่างๆ ที่เกี่ยวข้องในระบบ ISMS
- จัดทำและปรับปรุงทะเบียนทรัพย์สินในแต่ละส่วนงาน
- ประสานงานกับ ISMR/ISMA เพื่อทำการประเมินความเสี่ยงและบริหารจัดการความเสี่ยงสำหรับแต่ละส่วนงาน
- ประสานงานกับ ISMR/ISMA เพื่อดำเนินการตาม Security Plan ที่วางไว้
- ประสานงานกับ ISMR/ISMA เพื่อทำการวัดประสิทธิผลของกระบวนการและ Controls ในระบบ ISMS ที่เกี่ยวข้องในแต่ละส่วนงาน
- จัดทำ “บัญชีรายชื่อบันทึก” (Record List) และดำเนินการควบคุมบันทึกสำหรับแต่ละส่วนงาน

- ประสานงานกับ ISMR ในกรณีที่เกิดเหตุละเมิดความมั่นคง หรือเหตุฉุกเฉินใดๆ ขึ้นในบริษัทฯ เพื่อควบคุมและจัดการกับปัญหาที่เกิดขึ้น
- รับฟังข้อร้องเรียนหรือข้อเสนอแนะที่เกี่ยวข้องกับระบบ ISMS จากพนักงานและบุคคลภายนอกที่เกี่ยวข้อง และรายงานต่อ ISMR/ISMA ก่อนดำเนินการแก้ไขและป้องกัน เพื่อปรับปรุงการดำเนินงานของระบบ ISMS ให้มีประสิทธิภาพมากขึ้น

5.4. Document Controller

Document Controller คือ ผู้ทำหน้าที่ดูแลและควบคุมการใช้งานเอกสารและบันทึกต่างๆ ของระบบ ISMS ให้เป็นไปตามข้อกำหนดของมาตรฐาน ISO/IEC 27001 โดย Document Controller มีหน้าที่ความรับผิดชอบดังนี้

- ควบคุมและดูแลกระบวนการสร้างเอกสารขึ้นใหม่ แก้ไขเปลี่ยนแปลงเอกสาร และยกเลิกเอกสาร
- กำหนดเลขรหัสเอกสารและวันที่ของเอกสาร
- จัดเก็บต้นฉบับของเอกสาร หรือไฟล์ (Soft copy) ของเอกสาร
- จัดทำ Master List ของเอกสารระบบ ISMS ทั้งหมด และรับผิดชอบการปรับปรุงแก้ไขข้อมูลให้ถูกต้องอยู่เสมอ
- ควบคุมและดูแลให้เอกสารได้รับการทบทวนและปรับปรุงให้ทันสมัย ตามรอบเวลาอย่างเหมาะสม

5.5. Internal ISMS Auditor

Internal ISMS Auditor คือ ผู้ที่ได้รับมอบหมายให้ทำหน้าที่ตรวจประเมินภายในระบบ ISMS ของบริษัทเพื่อหาความสอดคล้องและข้อบกพร่อง เพื่อนำไปสู่การปรับปรุงระบบ ISMS อย่างต่อเนื่อง Internal ISMS Auditor มีหน้าที่ความรับผิดชอบดังนี้

- วางแผน ประสานงาน และดำเนินการตรวจประเมินภายในสำหรับระบบ ISMS ของบริษัทฯ
- รายงานผลการตรวจประเมิน พร้อมทั้งให้คำแนะนำในการปรับปรุงแก่ผู้ที่เกี่ยวข้อง
- ติดตามและตรวจสอบการดำเนินการแก้ไขหรือป้องกันข้อบกพร่องที่พบจากการตรวจประเมินภายใน

5.6. Asset Owner

Asset Owner มีหน้าที่ความรับผิดชอบในการจัดทำทะเบียนทรัพย์สิน กำหนดชั้นความลับสำหรับทรัพย์สินประเภทข้อมูล และทำให้มั่นใจว่าทรัพย์สินจะได้รับการปกป้องอย่างเหมาะสม ตลอดระยะเวลาการ

ใช้งานทรัพย์สิน รวมถึงดูแลความมั่นคงปลอดภัยที่เกี่ยวข้องกับการทำลาย จำหน่ายออก โอนย้าย หรือยกเลิกการใช้งานทรัพย์สิน

5.7. Risk Owner

Risk Owner มีหน้าที่ความรับผิดชอบในการประเมินความเสี่ยง วางแผนแก้ไขความเสี่ยง และทำให้มั่นใจว่าความเสี่ยงจะได้รับการแก้ไขตามแผน

5.8. Document Owner

Document Owner มีหน้าที่ความรับผิดชอบในการจัดทำ ทบทวน และปรับปรุงนโยบายการรักษาความมั่นคงปลอดภัยสารสนเทศ และเอกสารต่างๆ ที่เกี่ยวข้องในระบบ ISMS เพื่อให้มั่นใจว่าเอกสารมีความทันสมัยและสามารถนำไปใช้งานได้จริง Document Owner ต้องให้ความสนับสนุนในการประกาศใช้และปฏิบัติตามเอกสารเพื่อให้มั่นใจว่าบุคคลที่เกี่ยวข้องสามารถปฏิบัติงานตามเอกสารได้อย่างถูกต้อง โดยมีหน้าที่ดังนี้

- จัดทำ ทบทวน ปรับปรุง ยกเลิก และกำหนดเวอร์ชั่นของเอกสาร รวมถึงนำเอกสารไปขึ้นทะเบียนกับ Document Controller
- กำหนดชั้นความลับรวมถึงสิทธิ์การเข้าถึงเอกสารให้แก่ผู้เกี่ยวข้อง
- เรียกคืนและควบคุมเอกสารที่ยกเลิกการใช้งาน
- ควบคุมและดูแลให้มีการนำเอกสารไปใช้อย่างถูกต้องเหมาะสม รวมถึงควบคุมเมื่อมีการขอทำสำเนาเอกสาร

5.9. All personnel

พนักงานทุกคน รวมถึงบุคคลภายนอกที่เกี่ยวข้อง ผู้รับจ้าง ที่ปรึกษา พนักงานชั่วคราว คู่ค้า และผู้ให้บริการ ที่ใช้งานข้อมูลหรือระบบเทคโนโลยีสารสนเทศของบริษัทฯ มีหน้าที่ความรับผิดชอบดังนี้

- ปฏิบัติตาม รบ 1-2/2565 ระเบียบข้อบังคับเพื่อความปลอดภัยในการใช้งานระบบสารสนเทศ
- ปกป้องและดูแลรักษาข้อมูลและทรัพย์สินของบริษัทฯอย่างเหมาะสม มิให้มีการเข้าถึง แก้ไข เปิดเผย หรือทำลายโดยบุคคลที่ไม่ได้รับอนุญาต
- รับผิดชอบและปฏิบัติตามหน้าที่ที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยของข้อมูลและระบบเทคโนโลยีสารสนเทศที่ได้รับมอบหมายอย่างเหมาะสม
- รายงานสิ่งผิดปกติหรือจุดอ่อนด้านความมั่นคงปลอดภัยที่พบเห็นต่อบริษัทฯ อย่างเหมาะสม

6. การกำหนดวัตถุประสงค์และวางแผนการรักษาความมั่นคงปลอดภัยสารสนเทศ

6.1. การกำหนดวัตถุประสงค์ด้านความมั่นคงปลอดภัยสารสนเทศของบริษัทฯ

ทำการกำหนดวัตถุประสงค์ด้านความมั่นคงปลอดภัยสารสนเทศที่มีความสอดคล้องกับวัตถุประสงค์ทางธุรกิจ วัตถุประสงค์ที่กำหนดไว้ในนโยบายการรักษาความมั่นคงปลอดภัยสารสนเทศ และวัตถุประสงค์ของระบบ ISMS เพื่อกำหนดทิศทางในการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศภายในบริษัทฯ ให้สอดคล้องกับวัตถุประสงค์ทางธุรกิจ ความต้องการ และความคาดหวังของผู้ที่เกี่ยวข้อง

6.2. การวางแผนการรักษาความมั่นคงปลอดภัยสารสนเทศ

จัดทำแผนการรักษาความมั่นคงปลอดภัยสารสนเทศของบริษัทฯ เพื่อกำหนดกิจกรรมที่ต้องดำเนินการเพื่อให้บรรลุวัตถุประสงค์ด้านการรักษาความมั่นคงปลอดภัยสารสนเทศของบริษัทฯ ที่ได้กำหนดไว้

7. ระบบบริหารความมั่นคงปลอดภัยสารสนเทศ

ระบบบริหารความมั่นคงปลอดภัยสารสนเทศ หรือ ระบบ ISMS ของบริษัทฯ ได้รับการจัดตั้ง ใช้งาน ตรวจสอบ และปรับปรุงอย่างต่อเนื่อง ตามข้อกำหนดของมาตรฐาน ISO/IEC 27001 โดยใช้หลักการบริหารความเสี่ยง เพื่อสร้างความมั่นใจให้กับผู้ที่เกี่ยวข้องว่าข้อมูลและระบบสารสนเทศที่สำคัญของบริษัทฯ จะได้รับปกป้องอย่างเหมาะสม นอกจากนี้ระบบ ISMS ยังได้รับการออกแบบให้สามารถทำงานได้อย่างสอดคล้องกับกระบวนการและโครงสร้างการบริหารงานของบริษัทฯ โดยครอบคลุมกิจกรรมที่สำคัญดังต่อไปนี้

- การกำหนดความต้องการของบริษัทฯ ในการรักษาความมั่นคงปลอดภัยสารสนเทศ และการประกาศใช้งานนโยบายการรักษาความมั่นคงปลอดภัยสารสนเทศ รวมถึงการสื่อสารให้ผู้ที่เกี่ยวข้องรับทราบ
- การประเมินความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศของบริษัทฯ
- การสร้างมาตรการควบคุมที่สอดคล้องกับความเสี่ยงของบริษัทฯ
- การตรวจสอบและวัดผลการดำเนินงานและประสิทธิผลของระบบ ISMS
- การปรับปรุงอย่างต่อเนื่องที่สอดคล้องตามผลการวัดและวัตถุประสงค์ที่วางไว้

องค์ประกอบหลักของระบบ ISMS ของบริษัทฯแสดงได้ดังแผนภาพด้านล่างนี้

ภาพแสดงองค์ประกอบหลักของระบบ ISMS

การวิเคราะห์บริบทที่เกี่ยวข้องและการกำหนดขอบข่ายของระบบ ISMS (Context of the organization)

ทำการวิเคราะห์บริบทภายในและภายนอก รวมถึงความคาดหวังของผู้ที่เกี่ยวข้อง เพื่อกำหนดวัตถุประสงค์ด้านการรักษาความมั่นคงปลอดภัยสารสนเทศของบริษัทฯ และขอบข่ายของระบบ ISMS

บทบาทและหน้าที่ของผู้บริหาร (Leadership)

ให้ความสำคัญและให้การสนับสนุนการดำเนินงานของระบบ ISMS โดยการประกาศนโยบายการรักษาความมั่นคงปลอดภัยสารสนเทศ กำหนดหน้าที่ความรับผิดชอบของพนักงาน ทบทวนการดำเนินงานของระบบ ISMS และจัดสรรทรัพยากรที่จำเป็นในการดำเนินงานและปรับปรุงระบบ ISMS อย่างต่อเนื่อง

การวางแผนการดำเนินงานของระบบ ISMS (Planning)

ทำการวางแผนการรักษาความมั่นคงปลอดภัยสารสนเทศของบริษัทฯ เพื่อกำหนดกิจกรรมที่ต้องดำเนินการเพื่อให้บรรลุวัตถุประสงค์ด้านการรักษาความมั่นคงปลอดภัยสารสนเทศของบริษัทฯ ที่ได้กำหนดไว้ ตลอดจนทำการวิเคราะห์ความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศ รวมถึงความเสี่ยงที่อาจส่งผลต่อการดำเนินงานของระบบ ISMS และวางแผนแก้ไขความเสี่ยงโดยเลือกใช้มาตรการควบคุมที่เหมาะสมอย่างสมเหตุสมผล

การสนับสนุนการดำเนินงานของระบบ ISMS (Support)

ทำการบริหารทรัพยากรที่จำเป็นต่อการดำเนินงานของระบบ ISMS โดยเฉพาะอย่างยิ่งทรัพยากรบุคคลให้มีความรู้ความสามารถ และความตระหนักถึงความจำเป็นในการปฏิบัติตามนโยบายการรักษาความมั่นคงปลอดภัยสารสนเทศและกระบวนการของระบบ ISMS

การดำเนินงานของระบบ ISMS (Operation)

กำกับดูแลการดำเนินงานของระบบ ISMS และกิจกรรมการแก้ไขความเสี่ยงให้มีประสิทธิผลและเป็นไปตามแผนที่วางไว้ รวมถึงติดตามให้มีการประเมินความเสี่ยงและวางแผนแก้ไขความเสี่ยงอย่างสม่ำเสมอ หรือเมื่อมีความเปลี่ยนแปลงที่สำคัญที่อาจส่งผลต่อความเสี่ยงของบริษัทฯ

การประเมินประสิทธิผลของระบบ ISMS (Performance Evaluation)

ทำการตรวจสอบและประเมินประสิทธิผลของกระบวนการและมาตรการควบคุมต่างๆ เปรียบเทียบกับนโยบายการรักษาความมั่นคงปลอดภัยสารสนเทศ มาตรฐานที่เกี่ยวข้อง ตัวชี้วัด และวัตถุประสงค์ด้านการรักษาความมั่นคงปลอดภัยสารสนเทศของบริษัทฯ และรายงานผลต่อผู้บริหาร

การปรับปรุงระบบ ISMS อย่างต่อเนื่อง (Improvement)

ทำการแก้ไขข้อบกพร่องที่พบจากการตรวจสอบและประเมินประสิทธิผลของกระบวนการและมาตรการควบคุมต่างๆ รวมถึงทำการปรับปรุงระบบ ISMS อย่างต่อเนื่อง โดยการทบทวนและปรับปรุงวัตถุประสงค์ด้านการรักษาความมั่นคงปลอดภัยสารสนเทศของบริษัทฯ และแผนงานที่เกี่ยวข้อง

8. การสนับสนุนการดำเนินงานของระบบ ISMS

8.1. การจัดฝึกอบรม การให้ความรู้ และความสามารถของพนักงาน

ISMR/ISMA และผู้บังคับบัญชาต้นสังกัดต้องให้การสนับสนุนในการจัดฝึกอบรม ให้ความรู้แก่พนักงานที่เกี่ยวข้องที่ได้รับมอบหมายหน้าที่ความรับผิดชอบในระบบ ISMS อย่างเหมาะสมและเพียงพอต่อการปฏิบัติงาน โดย

- ระบุความสามารถที่จำเป็นสำหรับพนักงานที่ทำหน้าที่เกี่ยวข้องกับระบบ ISMS
- จัดให้มีการฝึกอบรม หรือจัดหาบุคลากรที่มีความรู้เข้าทำงาน (ในกรณีที่จำเป็น)
- ประเมินประสิทธิผลของการฝึกอบรม และดำเนินการตามความเหมาะสม

- จัดเก็บบันทึกของการฝึกอบรม ตลอดจนหลักฐานอื่นๆ ที่เป็นเครื่องยืนยันความรู้ความสามารถและประสบการณ์ของพนักงาน

ISMR/ISMA และผู้บังคับบัญชาต้นสังกัด ต้องทำให้พนักงานที่มีหน้าที่เกี่ยวข้องกับระบบ ISMS ตระหนักถึงความสำคัญของหน้าที่ความรับผิดชอบของตนในการรักษาความมั่นคงปลอดภัยของสารสนเทศ และช่วยให้บริษัทฯ ประสบความสำเร็จตามวัตถุประสงค์ที่กำหนดไว้

8.2. การสื่อสารภายในและภายนอก

จัดทำแผนการสื่อสาร (*ISMS-FM-38 Security Communication Plan*) เพื่อสื่อสารข้อมูลที่จำเป็นต่อการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศไปยังผู้ที่เกี่ยวข้องทั้งภายในและภายนอกบริษัทฯ

- การสื่อสารภายในบริษัทฯ หมายถึง การสื่อสารระหว่างส่วนงาน และการรายงานต่อผู้บริหาร
- การสื่อสารภายนอกบริษัทฯ หมายถึง การสื่อสารระหว่างบริษัทฯ กับหน่วยงานภายนอก เช่น คู่ค้า ผู้ให้บริการภายนอก หรือหน่วยงานภาครัฐที่เกี่ยวข้อง และการสื่อสารระหว่างบริษัทฯ กับบุคคลภายนอก เช่น ลูกค้า บุคคลทั่วไป เป็นต้น

8.3. การกำกับดูแลการปฏิบัติงานของผู้ให้บริการภายนอก

ทำการกำกับดูแลผู้ให้บริการภายนอกที่ดำเนินกิจกรรมหรือกระบวนการด้านการรักษาความมั่นคงปลอดภัยสารสนเทศให้แก่บริษัทฯ โดยควบคุมให้กิจกรรมหรือกระบวนการดังกล่าว เป็นไปตามนโยบายด้านการรักษาความมั่นคงปลอดภัยสารสนเทศของบริษัทฯ ตลอดจนเอกสารสนับสนุนอื่นๆ ที่เกี่ยวข้อง พร้อมทั้งทำการประเมินผลผู้ให้บริการภายนอกและสนับสนุนให้มีการปรับปรุงอย่างต่อเนื่อง

9. การบริหารจัดการความเสี่ยงและโอกาส

การบริหารจัดการความเสี่ยง คือกระบวนการที่เป็นระบบ ในการระบุความเสี่ยง ประเมินความเสี่ยง และ แก้ไขควบคุมความเสี่ยงให้อยู่ในระดับที่บริษัทฯ สามารถยอมรับได้ กระบวนการบริหารจัดการความเสี่ยงถือเป็นหัวใจสำคัญที่ทำให้ระบบ ISMS ของบริษัทฯ สามารถรักษาไว้ซึ่งความมั่นคงปลอดภัยสารสนเทศ โดยการบริหารจัดการความเสี่ยงเป็นงานที่ต้องดำเนินการอย่างต่อเนื่องเพื่อแก้ไขและควบคุมความเสี่ยงที่อาจเกิดขึ้นจากการเปลี่ยนแปลงทั้งจากภายในและภายนอกบริษัทฯ นอกจากการบริหารจัดการความเสี่ยงแล้วยังต้องคำนึงถึงโอกาส (Opportunity) ด้วย

มาตรฐานที่ใช้อ้างอิงในการบริหารจัดการความเสี่ยงของบริษัทฯ

- ISO 31000:2009, Risk Management – Principles and guidelines

- ISO/IEC 27005:2011, Information technology - Security techniques - Information security risk management
- NIST SP 800-30, Risk Management Guide for Information Technology Systems
- AS/NZS 4360

เกณฑ์ในการยอมรับความเสี่ยง และระดับความเสี่ยงที่สามารถยอมรับได้

บริษัทฯ จัดแบ่งระดับความเสี่ยงเป็น 4 ระดับ คือ H, S, M และ L โดยระดับความเสี่ยงที่บริษัทฯ สามารถยอมรับได้โดยไม่จำเป็นต้องดำเนินการแก้ไขและควบคุมความเสี่ยงคือ ระดับ L และ ระดับ M เท่านั้น การยอมรับความเสี่ยงที่เกินกว่าระดับ L และ ระดับ M ต้องดำเนินการอย่างเป็นลายลักษณ์อักษรและต้องได้รับความเห็นชอบจากผู้บริหารที่เกี่ยวข้อง โดยหลักเกณฑ์ในการยอมรับความเสี่ยงที่เป็นไปได้คือ

- การลงทุนเพื่อแก้ไขและควบคุมความเสี่ยงไม่คุ้มค่าเมื่อเทียบกับผลกระทบสูงสุดที่สามารถเกิดขึ้นได้
- ความเสี่ยงไม่สามารถแก้ไขและควบคุมให้ลดลงมาอยู่ในระดับ L หรือ ระดับ M ได้
- การตัดสินใจของผู้บริหารที่จะไม่ดำเนินการกับความเสี่ยงนั้น ซึ่งต้องมีเหตุผลสนับสนุนที่เหมาะสม

กระบวนการบริหารจัดการความเสี่ยงและโอกาส

กิจกรรมหลักของกระบวนการบริหารจัดการความเสี่ยงและโอกาสมี 3 ส่วนคือ

9.1. การประเมินความเสี่ยง (Risk Assessment) และ โอกาส (Opportunity Assessment)

การประเมินความเสี่ยง คือ การวิเคราะห์หาค่าความเสี่ยงโดยพิจารณาถึงเหตุการณ์ความเสี่ยง (Risk Scenario) ที่เป็นไปได้ โดยเหตุการณ์ความเสี่ยงนี้มีนัยครอบคลุมภัยคุกคาม (Threat) และจุดอ่อน (Vulnerability) ที่เกี่ยวข้อง จากนั้นจึงดำเนินการประเมินค่าความเป็นไปได้ (Likelihood) ที่จะเกิดความเหตุการณ์ความเสี่ยงขึ้น และประเมินค่าผลกระทบ (Impact) จากเหตุการณ์ความเสี่ยงนั้น โดยอ้างอิงตาม *ISMS-PC-06 Risk Assessment Procedure*

การประเมินโอกาส คือ การวิเคราะห์โอกาสที่เป็นไปได้ (Opportunity Scenario) และเป็นประโยชน์ต่อบริษัทฯ จากนั้นจึงดำเนินพิจารณาความเป็นไปได้ (Likelihood) และประเมินผลกระทบ (Impact) จากโอกาสนั้น

9.2. การแก้ไขและควบคุมความเสี่ยง (Risk Treatment)

การแก้ไขและควบคุมความเสี่ยง คือ การหาวิธีการหรือเครื่องมือต่างๆ ที่เหมาะสม เพื่อแก้ไขและควบคุมความเสี่ยงให้อยู่ในระดับที่บริษัทฯสามารถยอมรับได้ โดยมีแนวทางที่เป็นไปได้ในการแก้ไขและควบคุมความเสี่ยง ดังนี้

- แก้ไขความเสี่ยง
- ยอมรับความเสี่ยง
- หลีกเลี่ยงความเสี่ยง
- โอนหรือแบ่งปันความเสี่ยงกับหน่วยงานอื่น
- ยอมให้ความเสี่ยงเพิ่มขึ้น เพื่อโอกาสทางธุรกิจ

การเลือกแนวทางเพื่อแก้ไขและควบคุมความเสี่ยงต้องพิจารณาความเหมาะสมและทรัพยากรที่ต้องใช้ ทั้งนี้ การดำเนินการแก้ไขความเสี่ยง ให้อ้างอิงวิธีการแก้ไขจาก Controls ใน Annex A ของมาตรฐาน ISO/IEC 27001 โดยอ้างอิงตาม ISMS-PC-05 Risk Treatment Procedure

9.3. การทบทวนการประเมินความเสี่ยง (Review of Risk Assessment)

ผลการประเมินความเสี่ยงต้องได้รับการทบทวนตามรอบเวลาที่กำหนดไว้อย่างเหมาะสม อย่างน้อยปีละ 1 ครั้ง หรือเมื่อมีการเปลี่ยนแปลงที่สำคัญเกิดขึ้น เพื่อให้มั่นใจว่าวิธีการที่ใช้ และผลการประเมินความเสี่ยงสอดคล้องกับสถานการณ์ปัจจุบัน

10. การประเมินประสิทธิผล (Performance Evaluation)

การประเมินประสิทธิผล เป็นกระบวนการสำคัญที่แสดงให้เห็นถึงประสิทธิผล และการพัฒนาอย่างต่อเนื่องของระบบ ISMS ซึ่งช่วยให้บริษัทฯทราบว่า นโยบาย เอกสารสนับสนุน กระบวนการ มาตรการควบคุม และแนวทางการแก้ไขและควบคุมความเสี่ยงต่างๆ ที่เลือกใช้มีประสิทธิผลดีเพียงใด โดยทำการประเมินประสิทธิผลทั้งในส่วนของ ISMS Requirements (Clause 4 – 10) และ Controls ที่เลือกใช้งาน (Annex A) ของมาตรฐาน ISO/IEC 27001

ตัวชี้วัดที่ใช้ในการประเมินประสิทธิผล มีทั้งตัวชี้วัดก่อนเกิดเหตุ (Lead Indicator) และตัวชี้วัดหลังเกิดเหตุ (Lag Indicator) เพื่อให้ได้รับข้อมูลที่ครอบคลุม ผลที่ได้จากการประเมินประสิทธิผลจะถูกรายงานไปยังผู้บริหารและผู้ที่เกี่ยวข้อง เพื่อพิจารณาดำเนินการแก้ไขหรือปรับปรุงระบบ ISMS ต่อไป โดยอ้างอิงตาม *ISMS-PC-10 Effectiveness Measurement Procedure*

11. การตรวจประเมินภายในของระบบ ISMS

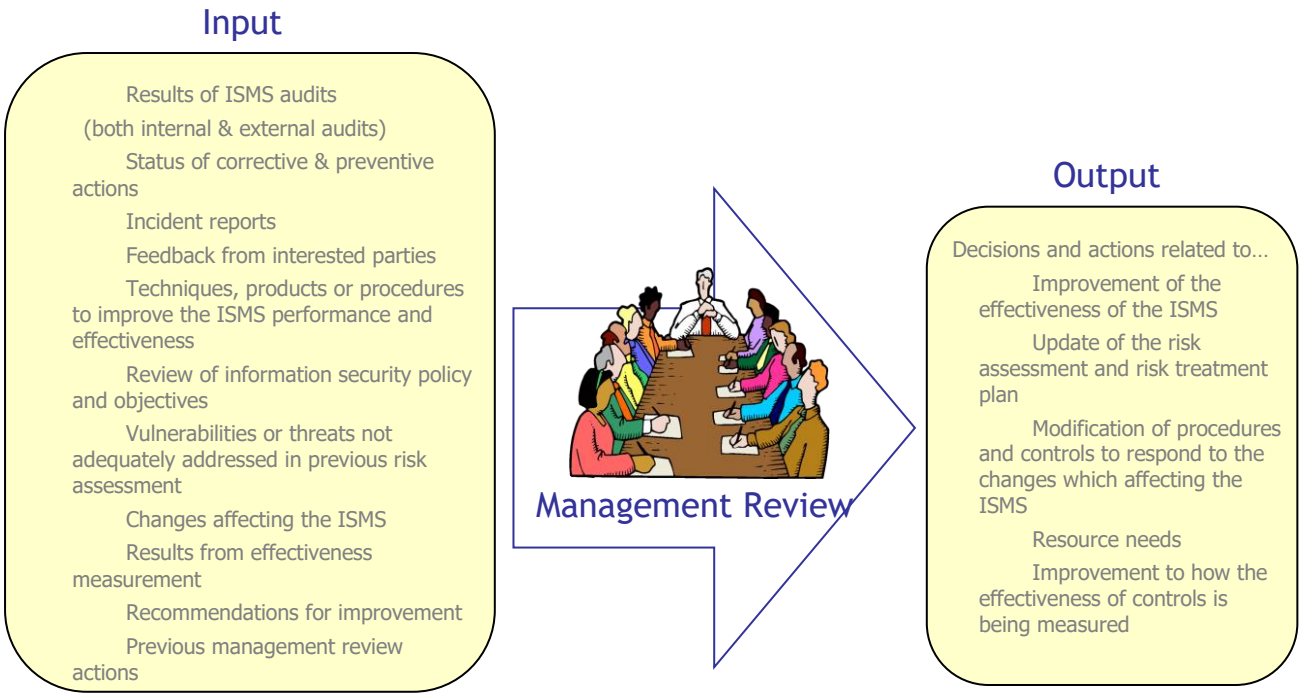
บริษัทฯ จัดให้มีการตรวจประเมินภายในสำหรับระบบ ISMS อย่างน้อยปีละ 1 ครั้ง เพื่อให้มั่นใจว่าการดำเนินงานของระบบ ISMS

- เป็นไปตามข้อกำหนดของมาตรฐาน ISO/IEC 27001 และ กฎหมาย กฎระเบียบต่างๆ ที่เกี่ยวข้อง
- เป็นไปตามข้อกำหนดและเอกสารของระบบ ISMS ของบริษัทฯ
- มีการนำไปปฏิบัติอย่างมีประสิทธิผล

การวางแผนการตรวจประเมินภายในต้องพิจารณาถึงความสำคัญของกระบวนการ ส่วนงาน หรือพื้นที่ที่จะทำการตรวจประเมิน และผลจากการตรวจประเมินในครั้งก่อน โดยผู้ทำการตรวจประเมินต้องได้รับการฝึกอบรม และคัดเลือกอย่างเหมาะสม มิให้มีการตรวจประเมินงานในส่วนที่ตนมีส่วนเกี่ยวข้อง ทั้งนี้ การวางแผน การดำเนินการตรวจประเมิน การรายงานผล และการติดตามทบทวนการแก้ไข ให้ปฏิบัติตาม IA-ISO-PC-01 Internal Audit Procedure โดยผู้บริหารของส่วนงานที่ถูกตรวจประเมินต้องให้ความร่วมมือในการหาสาเหตุและดำเนินการแก้ไขข้อบกพร่องที่ตรวจพบ

12. การทบทวนระบบ ISMS โดยผู้บริหาร

IT Sub-committee ต้องจัดประชุมเพื่อทบทวนการดำเนินงานของระบบ ISMS อย่างน้อยปีละ 1 ครั้ง เพื่อให้มั่นใจว่าการดำเนินงานของระบบ ISMS ของบริษัทฯ มีความเหมาะสม เพียงพอ และมีประสิทธิผล การทบทวนดังกล่าวต้องพิจารณาถึงโอกาสในการปรับปรุงระบบ ISMS และการเปลี่ยนแปลงต่างๆ ที่จำเป็นต้องดำเนินการ รวมถึงพิจารณาทบทวนและปรับปรุงนโยบายการรักษาความมั่นคงปลอดภัยสารสนเทศและวัตถุประสงค์ในการรักษาความมั่นคงปลอดภัยสารสนเทศของบริษัทฯ ทั้งนี้ ผลการทบทวนต้องได้รับการบันทึกไว้อย่างเหมาะสม



13. การดำเนินการแก้ไข

บริษัทฯ จัดให้มีกระบวนการดำเนินการแก้ไข (Corrective Action) เพื่อกำจัดสาเหตุของปัญหาหรือข้อบกพร่อง (Nonconformity) ที่พบในระบบ ISMS เพื่อป้องกันมิให้เกิดซ้ำ โดยการดำเนินการทั้งหมดต้องได้รับการสื่อสารไปยังพนักงานที่เกี่ยวข้องตามความเหมาะสม และมีการติดตามและตรวจสอบผลการดำเนินการเพื่อให้มั่นใจว่าบรรลุตามวัตถุประสงค์ของการดำเนินการ โดยอ้างอิงตาม *ISMS-PC-12 Corrective and Preventive Action Procedure*

14. Statement of Applicability (SOA)

Statement of Applicability หรือ SOA คือ เอกสารที่ระบุถึงการประยุกต์ใช้ Controls ทั้ง 114 ข้อของมาตรฐาน ISO/IEC 27001 ของบริษัทฯ โดยระบุถึง

- Controls ที่ได้เลือกใช้งานในระบบ ISMS พร้อมด้วยคำอธิบายของการประยุกต์ใช้งาน หรืออ้างอิงถึงเอกสารที่เกี่ยวข้องที่สามารถอธิบายการประยุกต์ใช้ Controls นั้นๆ ได้
- Controls ที่มิได้นำมาประยุกต์ใช้งาน พร้อมเหตุผลของการไม่นำมาใช้

15. การปรับปรุงระบบ ISMS อย่างต่อเนื่อง

บริษัทฯ ให้ความสำคัญต่อการปรับปรุงระบบ ISMS อย่างต่อเนื่อง เพื่อให้การรักษาความมั่นคงปลอดภัยสารสนเทศมีประสิทธิผล และสามารถปกป้องทรัพย์สิน ข้อมูล และระบบสารสนเทศที่สำคัญของบริษัทฯ จากภัยคุกคามที่มีการเปลี่ยนแปลงหรือเกิดขึ้นใหม่อยู่เสมอ โดยทำการทบทวนบริบทภายในและภายนอก ตลอดจนความต้องการและความคาดหวังของผู้ที่เกี่ยวข้อง เพื่อปรับปรุงวัตถุประสงค์ในการรักษาความมั่นคงปลอดภัยสารสนเทศและแผนการรักษาความมั่นคงปลอดภัยสารสนเทศของบริษัทฯ เป็นประจำทุกปี

16. เอกสารอ้างอิง

1. รบ.1-2/2565 ระเบียบข้อบังคับเพื่อความปลอดภัยในการใช้งานระบบสารสนเทศ
2. ISMS-PC-05 Risk Treatment Procedure
3. ISMS-PC-06 Risk Assessment Procedure
4. ISMS-PC-08 Document Control Procedure
5. ISMS-PC-09 Record Control Procedure
6. ISMS-PC-10 Effectiveness Measurement Procedure
7. ISMS-PC-12 Corrective and Preventive Action Procedure
8. IA-ISO-PC-01 Internal Audit Procedure
9. ISMS-FM-38 Security Communication Plan
10. ISMS-FM-40 Inventory of Assets Data Center

End of Document