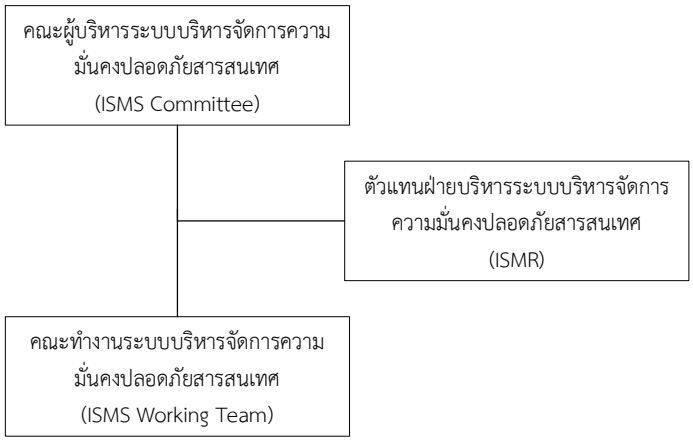


**1. คณะผู้บริหารระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ (ISMS Committee)**

คณะผู้บริหารระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ (ISMS Committee) มีหน้าที่ให้การสนับสนุนในการจัดตั้ง ในไปปฏิบัติ ตรวจสอบ และปรับปรุงระบบความมั่นคงปลอดภัยขององค์กร โดยมีหน้าที่ความรับผิดชอบดังนี้

- กำหนดทิศทางและเป็นที่ปรึกษาในการดำเนินงานระบบบริหารจัดการด้านความมั่นคงปลอดภัยสารสนเทศ
- พิจารณา อนุมัติและประกาศใช้งานนโยบายการรักษาความมั่งคงปลอดภัยสารสนเทศ
- พิจารณา อนุมัติและประกาศใช้งานเอกสารสารสนเทศต่าง ๆ ที่เกี่ยวข้องในระบบ
- สื่อสารให้พนักงานทุกคนตระหนักถึงความสำคัญของการรักษาความปลอดภัยข้อมูล และการปฏิบัติตามนโยบายการรักษาความมั่นคงปลอดภัยสารสนเทศและข้อกำหนดที่ระบุไว้ในเอกสารของระบบ ISMS
- ให้ความสนับสนุนในการให้ความรู้แก่พนักงานและบุคคลภายนอกที่เกี่ยวข้อง ให้รับทราบและสามารถปฏิบัติตามนโยบายการรักษาความปลอดภัยข้อมูลและข้อกำหนดที่ระบุไว้ในเอกสารที่เกี่ยวข้อง รวมถึงตรวจสอบการปฏิบัติตามของพนักงานและบุคคลภายนอกที่เกี่ยวข้อง
- พิจารณาลงโทษผู้ที่ละเมิดนโยบายการรักษาความมั่นคงปลอดภัยสารสนเทศและข้อกำหนดที่เกี่ยวข้อง
- กำหนดเกณฑ์ในการยอมรับความเสี่ยง และระดับความเสี่ยงที่ยอมรับได้ รวมถึงพิจารณาผลการประเมินความเสี่ยงและแผนการแก้ไขความเสี่ยงที่สำคัญขององค์กร
- ให้การสนับสนุนด้านทรัพยากรที่จำเป็นในการจัดทำ นำไปปฏิบัติ ตรวจสอบ และปรับปรุงระบบความมั่นคงปลอดสารสนเทศ
- ทบทวนการดำเนินงาน เพื่อให้มั่นใจว่าระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ มีความเหมาะสม และมีประสิทธิภาพ รวมถึงพิจารณาโอกาสในการปรับปรุงระบบให้ดีขึ้นอย่างต่อเนื่อง

**2. ตัวแทนฝ่ายบริหารระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ (ISMR)**

ตัวแทนของผู้บริหารขององค์กร ที่ทำหน้าที่ควบคุมดูแลการจัดตั้ง ใช้งาน ตรวจสอบ และปรับปรุงระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศขององค์กร โดยมีหน้าที่ความรับผิดชอบดังนี้

- ประสานงานเพื่อจัดตั้งและพัฒนาระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ ขึ้นในองค์กร รวมถึงดูแลรักษา ตรวจสอบ และปรับปรุงระบบอย่างต่อเนื่อง เพื่อให้บรรลุตามวัตถุประสงค์และนโยบาย ของระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ และสอดคล้องกับมาตรฐาน ISO/IEC 27001
- ดูแลการปรับปรุงแก้ไขนโยบาย และเอกสารต่าง ๆ ที่เกี่ยวข้อง ให้เหมาะสมเพียงพอกับการเปลี่ยนแปลงที่เกิดขึ้น สอดคล้องกับมาตรฐาน ISO/IEC 27001 และคำแนะนำที่ได้รับจากผู้บริหารขององค์กร
- สื่อสารให้พนักงานทุกคนรับทราบถึงหน้าที่และความรับผิดชอบของตนในการปฏิบัติตามนโยบายและเอกสารต่าง ๆ ที่เกี่ยวข้องของ
- ทบทวนการปฏิบัติงานขององค์กร ให้เป็นไปตามที่กำหนดไว้ในเอกสารต่าง ๆ ของระบบ
- ให้คำปรึกษาและแนะนำด้านการรักษาความมั่นคงปลอดภัยสารสนเทศและการนำนโยบายต่าง ๆ ไปใช้งาน
- บริหารการเปลี่ยนแปลงต่าง ๆ ที่เกิดขึ้นในบริษัท พร้อมทั้งประสานงานให้มีการประเมิน แก้ไขและควบคุมความเสี่ยงจากการเปลี่ยนแปลงอย่างเหมาะสม
- ควบคุมดูแลการวัดประสิทธิผลของกระบวนการและการควบคุมของระบบ
- ควบคุมดูแลการตรวจประเมินภายใน (Internal Audit) ให้เป็นไปตามที่ได้วางแผนไว้
- ควบคุมดูแลการดำเนินการแก้ไขและป้องกันข้อบกพร่องที่ตรวจพบ รวมถึงติดตามและทบทวนประสิทธิภาพของการแก้ไขและป้องกันอย่างเหมาะสม
- ประสานงานเพื่อจัดให้มีการประชุมเพื่อทบทวนผลการดำเนินงานโดยผู้บริหาร (Management Review) และติดตามการดำเนินการตามมติที่ประชุม

**3. คณะทำงานระบบบริหารจัดการด้านความมั่นคงปลอดภัยสารสนเทศ (ISMS Working Team)**

ประกอบด้วย ตัวแทนจากส่วนงานต่าง ๆ ที่อยู่ในขอบข่ายของระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ ทำหน้าที่ในการประสานงานและดำเนินงานของแต่ละส่วนงาน ซึ่ง มีหน้าที่ความรับผิดชอบดังนี้

- สื่อสาร ให้คำแนะนำ และดูแลพนักงานในแต่ละส่วนงาน เพื่อให้สามารถปฏิบัติงานได้อย่างถูกต้องตามนโยบายความมั่นคงปลอดภัยสารสนเทศและข้อกำหนดที่ระบุไว้ในเอกสารต่างๆ
- จัดทำและปรับปรุงทะเบียนทรัพย์สินที่เกี่ยวข้องภายใต้ขอบเขตของระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ
- ประสานงานกับตัวแทนฝ่ายบริหารระบบบริหารจัดการด้านความมั่นคงปลอดภัยสารสนเทศ (ISMR) เพื่อทำการประเมินความเสี่ยงและบริหารจัดการความเสี่ยง
- ประสานงานกับตัวแทนฝ่ายบริหารระบบบริหารจัดการด้านความมั่นคงปลอดภัยสารสนเทศ (ISMR) เพื่อทำการวัดประสิทธิผลของกระบวนการที่เกี่ยวข้อง

- จัดทำ “บัญชีรายชื่อบันทึก” (Record List) และดำเนินการควบคุมบันทึก
- ประสานงานกับตัวแทนฝ่ายบริหารระบบบริหารจัดการด้านความมั่นคงปลอดภัยสารสนเทศ (ISMR) ในกรณีที่เกิดเหตุละเมิดความความปลอดภัยสารสนเทศ หรือเหตุฉุกเฉิน เพื่อควบคุมและจัดการกับปัญหาที่เกิดขึ้น
- รับฟังข้อร้องเรียนหรือข้อเสนอแนะที่เกี่ยวข้องกับระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศจากพนักงานและบุคคลภายนอกที่เกี่ยวข้อง และดำเนินการแก้ไขและป้องกัน หรือรายงานต่อตัวแทนฝ่ายบริหารระบบบริหารจัดการด้านความมั่นคงปลอดภัยสารสนเทศ (ISMR) ปรับปรุงการดำเนินงานของระบบให้มีประสิทธิภาพมากขึ้น