

ระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ

Information Security Management System (ISMS)

ISO/IEC 27001: 2022

1. วัตถุประสงค์

นโยบายฉบับนี้ จัดทำขึ้นเพื่อเป็นแนวทางหลักในการดำเนินกิจกรรมในระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ ของบริษัท ไอรา พร็อพเพอร์ตี้ จำกัด (มหาชน) โดยการกำหนดนโยบายระดับสูง หน้าที่ความรับผิดชอบที่จำเป็นในการดำเนินกิจกรรม และรายการกิจกรรมในระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ

2. นโยบายสำหรับระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ

2.1 ข้อกำหนดด้านความมั่นคงปลอดภัยสารสนเทศ

ในการดำเนินงานบนระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศนั้น จะต้องเป็นไปตามข้อกำหนดด้านความมั่นคงปลอดภัยในแต่ละด้าน ดังต่อไปนี้

ข้อกำหนดตามการกำหนดค่าเป้าหมายและการรายงานผลการปฏิบัติงานตามตัวชี้วัด (KPI)

ระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ จำเป็นต้องวัดผลประสิทธิภาพได้ โดยใช้ตัวชี้วัดที่มีความสอดคล้องกับนโยบายหน่วยงาน ความเสี่ยง ตลอดจนการวัดผลประสิทธิภาพของมาตรการควบคุมเชิงความปลอดภัยสารสนเทศที่บริษัท ไอรา พร็อพเพอร์ตี้ จำกัด (มหาชน) ได้นำมาใช้ ทั้งนี้ ผลประสิทธิภาพต้องได้รับการ รายงานแก่คณะผู้บริหารและสื่อสารไปถึงทุกหน่วยงานที่เกี่ยวข้อง โดยกำหนดให้การวัดผลประสิทธิภาพของระบบ บริหารจัดการความมั่นคงปลอดภัยสารสนเทศต้องทำขึ้นอย่างน้อย 1 ครั้งต่อปี โดยตัวชี้วัดต้องครอบคลุมทุกหน่วยงาน ภายใต้ขอบเขตการดำเนินงาน

ข้อกำหนดเชิงกฎหมาย

ระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ จำเป็นต้องมีความสอดคล้องตามข้อกำหนดกฎหมาย กฎระเบียบ ข้อบังคับ ตลอดจนนโยบายทั้งภายในและภายนอกบริษัท ไอรา พร็อพเพอร์ตี้ จำกัด (มหาชน) ที่มีส่วนเกี่ยวข้อง ทั้งโดยตรงและโดยอ้อม ในการดำเนินกิจกรรม โดยเป็นหน้าที่สำคัญของบุคลากรทุกคนภายใต้ขอบเขตการดำเนินงานที่ต้องศึกษาทำความเข้าใจกับข้อกำหนดต่างๆ

ทั้งนี้ รายการข้อกำหนดที่เกี่ยวข้องกับระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ ได้แก่

- พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.2550 และฉบับแก้ไขเพิ่มเติม
- พระราชบัญญัติลิขสิทธิ์ พ.ศ. 2537 และฉบับแก้ไขเพิ่มเติม
- พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562
- พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

อ้างอิง: เอกสารรายการประเมินความสอดคล้องข้อกำหนด (Legal)

ข้อกำหนดตามมาตรฐานสากล ISO/IEC 27001: 2022

ระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ ต้องมีความสอดคล้องกับข้อกำหนดตามมาตรฐานสากล ISO/IEC 27001: 2022 ทั้งในส่วนของการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ และรายการมาตรการควบคุมที่นำมาใช้

อ้างอิง: เอกสารรายการมาตรการด้านความมั่นคงปลอดภัยสารสนเทศที่นำมาประยุกต์ใช้ (Statement of Applicability)

2.2 หลักการด้านความมั่นคงปลอดภัยสารสนเทศ

ระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ ใช้แนวทางด้านความมั่นคงปลอดภัยของข้อมูล โดยพิจารณาองค์ประกอบ 3 ข้อหลัก ได้แก่

องค์ประกอบ	คำอธิบาย
ความลับ (Confidentiality)	การรักษาไว้ซึ่งความลับของสารสนเทศไม่ถูกเปิดเผยแก่ระบบ คน และ/หรือ หน่วยงานที่ไม่ได้มีส่วนเกี่ยวข้อง
ความสมบูรณ์ (Integrity)	การรักษาไว้ซึ่งความถูกต้อง เสถียรภาพของสารสนเทศไม่ถูกแก้ไข หรือนำไปใช้อย่างผิดวิธี และสามารถตรวจสอบความถูกต้องของสารสนเทศก่อนการนำไปใช้งานได้
ความพร้อมใช้ (Availability)	การรักษาไว้ซึ่งความพร้อมใช้งานของสารสนเทศ

โดยองค์ประกอบข้างต้น จะถูกนำมาพิจารณาเป็นมูลค่าของทรัพย์สินสารสนเทศในเชิงความมั่นคงปลอดภัย อันรวมถึงทรัพย์สินอื่นๆ ที่เกี่ยวข้องกับสารสนเทศ

ความมั่นคงปลอดภัยสารสนเทศบนพื้นฐานของความเสี่ยง (Information Security aspects to risk based approach)

ระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ ยึดแนวทางการพิจารณาความเสี่ยงที่มีผลกระทบต่อทรัพย์สินสารสนเทศ ทั้งทางตรงและทางอ้อม ผ่านการประเมินมูลค่าความเสียหายและโอกาสการเกิดขึ้นของภัยคุกคาม ที่อาศัยช่องโหว่ของทรัพย์สินหรือระบบสารสนเทศที่ไม่มีประสิทธิภาพ

อ้างอิง: เอกสารระเบียบขั้นตอนการบริหารจัดการความเสี่ยง (Risk Management Methodology)

2.3 เป้าหมายของความมั่นคงปลอดภัยสารสนเทศ

เป้าหมายสำคัญของการดำเนินกิจกรรมตามระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ คือการลดและหลีกเลี่ยงปัญหาการละเมิดความมั่นคงปลอดภัยสารสนเทศ อันส่งผลต่อภาพลักษณ์และความเชื่อมั่นของลูกค้าเพื่อให้ได้รับรองมาตรฐานสากลด้านความมั่นคงปลอดภัยสารสนเทศอย่างต่อเนื่องในการดำเนินงานด้วยระบบเทคโนโลยีสารสนเทศที่มีความมั่นคงปลอดภัย (Information Security)

2.4 การจัดทำกลยุทธ์ด้านความมั่นคงปลอดภัยสารสนเทศ

กลยุทธ์ด้านความมั่นคงปลอดภัยมีการกำหนดขึ้นเพื่อสร้างกรอบการปฏิบัติแก่ผู้ปฏิบัติงาน ภายใต้ขอบเขต โดยการเข้าใจถึงวัตถุประสงค์และแนวทางที่สามารถใช้ในการดำเนินกิจกรรม โดยมีการกำหนดกลยุทธ์ดังต่อไปนี้

ความสามารถในการปรับเปลี่ยนเพื่อสร้างความสอดคล้อง (Flexibility)

ระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศถูกออกแบบให้มีความเหมาะสมกับสภาวะแวดล้อมของบริษัท ไอรา พร็อพเพอร์ตี้ จำกัด (มหาชน) สามารถเปลี่ยนแปลงตามปัจจัยต่างๆ เพื่อให้ผู้ปฏิบัติงานสามารถนำระบบสารสนเทศ ไปใช้งานได้อย่างจริง ไม่ก่อให้เกิดความยากลำบากในการดำเนินงานหรือใช้เวลาจากงานเกินพอดี

ระบบบริหารจัดการความมั่นคงปลอดภัยบนพื้นฐานของความเสี่ยง (Risk based approach)

บริษัท ไอรา พร็อพเพอร์ตี้ จำกัด (มหาชน) ต้องพิจารณาถึงความเสี่ยงด้านข้อมูลสารสนเทศเป็นสำคัญ เพื่อพิจารณาถึงการเลือกใช้มาตรการควบคุมหรือการกำหนดนโยบายต่างๆ ให้เกิดความสอดคล้อง โดยให้มุ่งเน้นถึงผลกระทบในทุกด้านที่เกี่ยวข้อง และระดับการควบคุมป้องกันภัยคุกคามที่เหมาะสม

การส่งเสริมศักยภาพบุคลากร และทักษะที่จำเป็นในการรับมือความมั่นคงปลอดภัยสารสนเทศ

ไอรา พร็อพเพอร์ตี้ จำกัด (มหาชน) ต้องมั่นใจว่าบุคลากรภายใต้ขอบเขตระบบบริหารจัดการ ความมั่นคงปลอดภัยสารสนเทศ มีทักษะความสามารถเพียงพอต่อการทำกิจกรรมต่างๆ โดยทักษะความสามารถ แบ่งออกเป็น

- ทักษะเฉพาะทางและความชำนาญพิเศษตามสายงาน
 - การดูแลรักษาเครื่องคอมพิวเตอร์แม่ข่าย ระบบสนับสนุนโครงสร้างพื้นฐาน และระบบเครือข่ายเพื่อความมั่นคงปลอดภัยการบริหารจัดการ Supplier การรองรับเหตุการณ์ละเมิดความมั่นคงปลอดภัย การเก็บรวบรวมหลักฐานทางด้านไอที
 - การบริหารจัดการความต่อเนื่องทางธุรกิจ (Business Continuity Management)
- ทักษะด้านความมั่นคงปลอดภัยสารสนเทศและระบบฯ
 - ความเข้าใจในระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ
 - ความเข้าใจในกระบวนการบริหารจัดการความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศ

2.5 การกำกับดูแลและหน้าที่ความรับผิดชอบ

คณะกรรมการบริหารความมั่นคงปลอดภัยสารสนเทศ (ISMS Committee)

คณะกรรมการบริหารความมั่นคงปลอดภัยสารสนเทศ (ISMS Committee) มีหน้าที่ในการวางแผนจัดการ สนับสนุนให้ทุกกิจกรรมที่เกี่ยวข้องกับความมั่นคงปลอดภัยสารสนเทศเป็นไปตามข้อกำหนดนโยบาย ทั้งนี้ คณะกรรมการบริหารความมั่นคงปลอดภัยสารสนเทศ (ISMS Committee) ต้องดำเนินการดังต่อไปนี้

- ตรวจสอบและอนุมัติกรอบการดำเนินงานและนโยบายด้านความมั่นคงปลอดภัยสารสนเทศ
- กำหนดทิศทางและให้คำปรึกษาในการสร้าง รวมถึงพัฒนาระบบการรักษาความมั่นคงปลอดภัย สารสนเทศกำหนด เป้าหมายและวัตถุประสงค์ของการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ
- สนับสนุนทรัพยากรที่จำเป็นเพื่อให้บรรลุวัตถุประสงค์ด้านความมั่นคงปลอดภัยสารสนเทศที่ หน่วยงานกำหนดไว้
- พิจารณาและอนุมัติวิธีการบริหารจัดการความเสี่ยง (Risk Management Methodology) และระดับความเสี่ยงที่หน่วยงาน ยอมรับได้ (Acceptable Risk Level หรือ ARL)
- พิจารณาแผนการดำเนินการจัดการความเสี่ยงและความเสี่ยงที่เหลืออยู่ รวมถึงอนุมัติกรอบการ บริหารจัดการความ ต่อเนื่องของธุรกิจให้สอดคล้องกับเป้าหมายของหน่วยงาน

- ให้คำปรึกษาในการดำเนินงานระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ (ISMS) ตามมาตรฐาน ISO/IEC 27001: 2022
- ปรับปรุงข้อกำหนด ข้อกำหนดที่เกี่ยวข้องกับขอบเขตระบบบริหารจัดการความมั่นคงปลอดภัย สารสนเทศ (ISMS Scope) ให้มีความเหมาะสม
- ดำรงตำแหน่งเป็นเจ้าของความเสี่ยง (Risk Owner) มีอำนาจในการพิจารณาอนุมัติแผนการจัดการความเสี่ยง ผลการประเมิน ตลอดจนแนวทางมาตรการที่เหมาะสม ทั้งนี้ผู้บริหารสามารถมอบหมาย หน้าที่ความรับผิดชอบในการดูแลความเสี่ยงให้แก่ ISMR หรือผู้ที่ได้รับการแต่งตั้งได้
- ทบทวนการบริหารจัดการระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ (ISMS Management Review)
- ทบทวนและอนุมัติ กรณียุติและมาตรฐานที่มีอยู่ไม่ครอบคลุมความเสี่ยงดังกล่าว
- อนุมัติความเสี่ยงคงเหลือ (Residual Risk) ในระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ
- มีอำนาจแต่งตั้งคณะทำงานบริหารจัดการด้านความมั่นคงปลอดภัยสารสนเทศ (ISMS Working Team) เจ้าหน้าที่ดูแลเอกสาร (Document Control Officer) และ คณะผู้ตรวจสอบภายในระบบ บริหารจัดการความมั่นคงปลอดภัยสารสนเทศ (ISMS Internal Audit)

ผู้บริหารจัดการด้านความมั่นคงปลอดภัยสารสนเทศ (ISMS Management Representative: ISMR)

ผู้บริหารจัดการด้านความมั่นคงปลอดภัยสารสนเทศ (ISMR) มีหน้าที่รายงานผลการดำเนินการต่อคณะกรรมการบริหารความมั่นคงปลอดภัยสารสนเทศ (ISMS Committee) โดยมีความรับผิดชอบดังต่อไปนี้

- ควบคุมและแก้ไขปัญหาให้การบริหารจัดการความมั่นคงปลอดภัยข้อมูลสารสนเทศ ถูกนำไปใช้ได้ อย่างมีประสิทธิภาพ
- รายงานประสิทธิภาพการดำเนินงานของระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ (ISMS) ต่อคณะกรรมการ ISMS Committee ในขั้นตอนการทบทวนของฝ่ายบริหาร หรือ Management Review Meeting
- ดำเนินการร่วมกับคณะตรวจประเมินภายใน ในการติดต่อกับหน่วยงานที่ให้การรับรอง เพื่อวางแผน และกำหนดแผนในการตรวจประเมินระบบ ISMS ตามมาตรฐาน ISO/IEC 27001: 2022
- ติดตามการดำเนินการและการปฏิบัติงานของระบบ ISMS ในการใช้งานจริงและประสานกับผู้ที่เกี่ยวข้องในการเฝ้าระวังรักษา ทบทวน และปรับปรุงระบบ ISMS
- ตรวจสอบผลการดำเนินการ รวมถึงดำเนินงานร่วมกับคณะทำงาน ISMS เพื่อประเมินประสิทธิภาพ และความสอดคล้องของระบบ ISMS
- รับผิดชอบในการนำระบบ ISMS ไปใช้งานจริงและดูแลให้การนำไปใช้งานเป็นไปตามวัตถุประสงค์ ของการจัดทำระบบ ISMS
- ดำรงตำแหน่งเป็นเจ้าของความเสี่ยง (Risk Owner) เมื่อได้รับการแต่งตั้งหรือมอบหมายจากคณะ ผู้บริหาร
- ปฏิบัติหน้าที่อื่นๆ ตามที่ได้รับมอบหมายจากคณะบริหารความมั่นคงปลอดภัยสารสนเทศ

คณะทำงานบริหารจัดการด้านความมั่นคงปลอดภัยสารสนเทศ (ISMS Working Team)

คณะทำงาน ISMS คือผู้ประสานงานผู้บริหารจัดการด้านความมั่นคงปลอดภัยสารสนเทศ (ISMR) โดยให้คำแนะนำการดำเนินงานที่เกี่ยวข้องกับความมั่นคงปลอดภัยสารสนเทศในบริษัท ไอรา พร็อพเพอร์ตี้ จำกัด (มหาชน) ซึ่งมีความรับผิดชอบดังต่อไปนี้

- เป็นผู้แทนหน่วยงานในการร่วมมือและนำระบบ ISMS ไปปฏิบัติในหน่วยงานของตน

- ดำเนินการตามนโยบายด้านการบริหารจัดการความมั่นคงปลอดภัยข้อมูลสารสนเทศ
- อบรมและสร้างความตระหนักด้านการรักษาความมั่นคงปลอดภัยสารสนเทศให้แก่พนักงานในหน่วยงาน
- ดำเนินการประเมินความเสี่ยงตามกระบวนการที่หน่วยงานกำหนดไว้
- รายงานการดำเนินงานต่อผู้แทนกรรมการบริหารจัดการความมั่นคงปลอดภัยข้อมูลสารสนเทศ (ISMR) และนำระบบ ISMS มาปฏิบัติใช้
- สนับสนุนและดูแลให้มีการนำนโยบายด้านความมั่นคงปลอดภัยมาใช้อย่างเหมาะสม
- ตรวจสอบและปรับปรุงแก้ไขกระบวนการอย่างสม่ำเสมอให้มีความเหมาะสมและมีประสิทธิภาพ
- ให้คำแนะนำและชี้แจงเพื่อให้พนักงานและบุคคลที่เกี่ยวข้องปฏิบัติตามข้อกำหนดและเป็นไปตาม มาตรฐาน ISO/IEC 27001: 2022 รวมถึงข้อกฎหมายและข้อบังคับที่เกี่ยวข้อง
- ดำเนินการจัดทำ ติดตาม และปรับปรุงแผนการสื่อสารของระบบ ISMS
- ดำเนินการจัดทำ ติดตาม และตรวจสอบผลการดำเนินการตามตัวชี้วัดประสิทธิภาพของระบบ ISMS
- ร่วมกิจกรรมการประเมินความเสี่ยงของทรัพย์สินสารสนเทศของหน่วยงานที่เกี่ยวข้อง
- ติดตามและตรวจสอบการเปลี่ยนแปลงของภัยคุกคามที่สำคัญที่เกี่ยวข้องกับทรัพย์สินสารสนเทศที่มีความเสี่ยง
- รายงานและวิเคราะห์เหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัยสารสนเทศพร้อมดำเนินการแก้ไขและป้องกันการเกิดซ้ำ
- แก้ไขและกำหนดวิธีการป้องกันเพื่อให้ระบบ ISMS ดำเนินการไปตามนโยบายที่องค์กรกำหนดไว้ ชี้แจงและให้ความรู้แก่บุคลากร ตลอดจนผู้ให้บริการและบำรุงรักษา (Vendor) ที่เกี่ยวข้องให้สามารถปฏิบัติตามข้อกำหนด นโยบาย ข้อกฎหมาย และข้อบังคับอื่นๆ ที่เกี่ยวข้องได้อย่างถูกต้อง
- ประสานงานระหว่างคณะกรรมการและหน่วยงานอื่นที่เกี่ยวข้อง เพื่อดำเนินการให้ได้ตามที่กำหนดไว้ในระบบ ISMS
- ปฏิบัติหน้าที่อื่นๆ ตามที่ได้รับมอบหมายจากคณะบริหารความมั่นคงปลอดภัยสารสนเทศ

คณะตรวจประเมินภายใน (Internal Auditor)

คณะตรวจประเมินภายในจะเป็นผู้ตรวจสอบผลการดำเนินงานด้านการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ ตลอดจนกระบวนการต่างๆ เพื่อให้มั่นใจว่าสอดคล้องกับนโยบายด้านความมั่นคงปลอดภัย สารสนเทศและมาตรฐานข้อกำหนดที่เกี่ยวข้อง โดยมีหน้าที่ความรับผิดชอบ ดังนี้

- จัดเตรียมแผนการตรวจประเมิน
- จัดให้มีกิจกรรมการตรวจประเมินตามแผนที่กำหนดไว้
- จัดอบรมผู้ตรวจประเมินให้มีความรู้ความสามารถในการปฏิบัติงานได้อย่างเหมาะสม
- ดำเนินการตรวจประเมินและจัดทำรายงานผลการตรวจประเมิน
- ติดตามและตรวจสอบผลการแก้ไขและการป้องกัน
- รายงานผลการตรวจประเมินภายในของระบบ ISMS ต่อคณะกรรมการ ISMS Committee
- ดำเนินการร่วมกับ ISMR ในการติดต่อกับหน่วยงานที่ให้การรับรอง เพื่อวางแผนและ กำหนดแผนในการตรวจประเมินระบบ ISMS ตามมาตรฐาน ISO/IEC 27001: 2022

เจ้าของระบบ (System Owner)

เจ้าของระบบ คือ บุคคลซึ่งได้รับมอบหมายให้จัดการข้อมูลสารสนเทศในระบบงานของตนเองโดยเจ้าของระบบสารสนเทศ จะต้องเป็นผู้ร่วมกำหนดนโยบายสนับสนุนด้านความมั่นคงปลอดภัยระบบสารสนเทศ ตลอดจนตรวจทานและรับรองสิทธิการเข้าใช้ระบบงานตาม ขอบเขตที่รับผิดชอบ ให้เหมาะสมกับระดับชั้นความลับของข้อมูล

ผู้ดูแลระบบ (Custodian)

ผู้ดูแลระบบ คือ บุคคลซึ่งได้รับมอบหมายให้บริหารจัดการระบบสารสนเทศจากเจ้าของระบบ (System Owner) โดยจะต้องปฏิบัติตามนโยบายด้านความมั่นคงปลอดภัยระบบสารสนเทศของการให้บริการและขั้นตอนการปฏิบัติงานด้านการรักษาความมั่นคงปลอดภัยที่กำหนดไว้ และดูแลให้ระบบสารสนเทศดังกล่าวสามารถให้บริการได้สอดคล้องกับข้อกำหนดในนโยบายด้าน ความมั่นคงปลอดภัยด้วย ทั้งนี้การเพิ่มหรือเพิกถอนสิทธิ์ในการเข้าถึงระบบใดๆ ให้ปฏิบัติตามคู่มืออำนาจดำเนินการกำหนดอย่างเคร่งครัด ตลอดจนทบทวนความเหมาะสมของมาตรการที่นำมาใช้ พร้อมทั้งรายงานผลการดำเนินงานให้เจ้าของระบบ (System Owner) ทราบเป็นระยะ

ผู้ใช้ (User)

ผู้ใช้ได้แก่ บุคคล (หรือบางครั้งอาจหมายถึงระบบสารสนเทศหรือกระบวนการ) ที่ได้รับอนุญาตให้สามารถเข้าถึงข้อมูลสารสนเทศได้ตามกระบวนการหรือข้อบังคับของเจ้าของระบบเอง อย่างไรก็ตามผู้ใช้งานจะต้องปกป้องข้อมูลภายใต้การควบคุมของผู้ดูแลระบบและจะต้องปฏิบัติตามข้อกำหนดในนโยบายมาตรฐานและแนวทางการดำเนินงานที่เกี่ยวข้อง ทั้งนี้ผู้ใช้งานจะต้องรับผิดชอบการดำเนินการใดๆ ที่เกี่ยวข้องกับการใช้งานข้อมูลสารสนเทศ หากทราบหรือสงสัยมีการละเมิดนโยบายความมั่นคงปลอดภัยสารสนเทศ จะต้องรายงานต่อผู้บังคับบัญชา หรือผู้บริหารจัดการ ด้านความมั่นคงปลอดภัยสารสนเทศ (ISMR) โดยทันที

3. กรอบการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ

กรอบการดำเนินงานสำหรับระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ (ISMS Framework) ใช้โมเดล Plan-Do-Check-Act (PDCA) ในการจัดทำระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ ซึ่งสามารถสรุปกิจกรรมการดำเนินการต่างๆ ดังต่อไปนี้



3.1 กิจกรรมวางแผน (Plan)

รายละเอียดของกิจกรรมนี้ ประกอบไปด้วยกระบวนการ 5 ขั้นตอน ดังนี้

3.1.1 กำหนดขอบเขต วัตถุประสงค์ และแต่งตั้งคณะกรรมการที่เกี่ยวข้อง

- การกำหนดขอบเขตของการนำระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ ให้สอดคล้องกับและวัตถุประสงค์ของบริษัท ไอรา พร็อพเพอร์ตี้ จำกัด (มหาชน)

- การกำหนดปัจจัยและปัญหาที่นำมาสู่การดำเนินกิจกรรมในระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศของบริษัท ไอรา พร็อพเพอร์ตี้ จำกัด (มหาชน)
- แต่งตั้งคณะกรรมการทางด้าน ISMS เพื่อร่วมขับเคลื่อนระบบ ISMS ภายใต้ขอบเขตที่กำหนดไว้
- จัดทำเอกสารนโยบายระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ ซึ่งจะกำหนดวิสัยทัศน์ พันธกิจ วัตถุประสงค์ ตลอดจนหน้าที่ความรับผิดชอบของคณะกรรมการที่เกี่ยวข้องกับการดำเนินการระบบ ISMS และเอกสารขอบเขตระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ

3.1.2 กำหนดโครงสร้างเอกสารและนโยบายความปลอดภัยของข้อมูล

- กำหนดโครงสร้างเอกสารระบบ ISMS เพื่อใช้ควบคุมเอกสารต่างๆ ที่อยู่ในระบบ และแสดงถึงลำดับความสำคัญของเอกสารในแต่ละระดับสำหรับรายละเอียดในส่วนนี้จะถูกอธิบายไว้ในระเบียบขั้นตอนการควบคุมเอกสาร (Document Control Procedure)
- นโยบายระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ (ISMS Policy) จะประกอบไปด้วยหลักการด้านความมั่นคงปลอดภัยสารสนเทศซึ่งจะต้องได้รับการทบทวนและอนุมัติโดยผู้มีอำนาจ (Top management)

3.1.3 กำหนดขอบเขตการดำเนินงาน ISMS

- กำหนดบริการที่ต้องการจะรับการตรวจสอบเพื่อขอรับใบรับรอง (Certify) โดยต้องอยู่ในขอบเขตที่กำหนดไว้
- การกำหนดบริการและระบบสารสนเทศรวมทั้งรายการทรัพย์สินสารสนเทศภายในขอบเขตของการดำเนินงานจะพิจารณาตามประเด็นบริการด้านเทคโนโลยีสารสนเทศที่มีผลต่อภารกิจของบริษัท ไอรา พร็อพเพอร์ตี้ จำกัด (มหาชน)
- ข้อมูลดังกล่าวข้างต้นจะถูกจัดเก็บไว้ในรายการบัญชีทรัพย์สิน

3.1.4 กำหนดวิธีประเมินความเสี่ยงและการจัดการความเสี่ยง

- วิธีที่ใช้ในการประเมินและการบริหารความเสี่ยงนั้นได้นำกระบวนการ ควบคุมความเสี่ยง ตามมาตรฐานมาประยุกต์ใช้

3.1.5 กำหนดตัวชี้วัด

- ต้องมีการกำหนดตัวชี้วัดเพื่อประเมินประสิทธิภาพของมาตรการต่างๆ ที่นำมาใช้
- ตัวชี้วัดจะต้องเป็นการวัดผลเชิงปริมาณโดยตัวชี้วัดดังกล่าวจะต้องมีองค์ประกอบ ดังต่อไปนี้
 - เป้าหมายการนำไปใช้งาน (Objective of the metrics)
 - การวัดและวิเคราะห์ผล (Measurement of the Metrics)
 - วัตถุประสงค์การนำไปใช้ (Purpose of metrics)
 - ความถี่ในการเก็บข้อมูล (Frequency)
 - การคำนวณค่าของตัวชี้วัด (Process Method)
- ต้องจัดทำเอกสารอ้างอิงเพื่อสนับสนุนการเก็บรวบรวมและวิเคราะห์ในเมตริกตัวชี้วัดตัวเดียวกันอาจนำไปใช้สำหรับมาตรการอื่นๆ ได้หาก หากข้อมูลที่ได้จากตัวชี้วัดดังกล่าวสามารถนำไปใช้วัดผล

วัตถุประสงค์ของมาตรการดังกล่าวได้

3.2 กิจกรรมดำเนินการ (Do)

รายละเอียดของขั้นตอนดำเนินการ (Do) ของกรอบวิธีดำเนินการระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ (ISMS Framework) เป็นดังต่อไปนี้

3.2.1 การประเมินความเสี่ยงและการจัดการความเสี่ยง

- ผู้ดูแลระบบและเจ้าของระบบสารสนเทศที่อยู่ในขอบเขตการดำเนินงาน ระบบ ISMS จะทำการตรวจสอบทรัพย์สินของตนเอง ประเมินผลการกระทบ และความเสี่ยงของทรัพย์สินตามแนวทางการประเมินความเสี่ยง
- กำหนดระดับความเสี่ยงที่ยอมรับได้ (ARL) โดยเปรียบเทียบกับความเสี่ยงในปัจจุบันและดำเนินการลดความเสี่ยงสำหรับทรัพย์สินที่มีค่าความเสี่ยงมากเกินไปกว่าค่าที่ยอมรับได้ (Overexposed Assets)

3.2.2 จัดทำเอกสารรายการข้อกำหนดที่นำมาใช้ (Statement of Applicability)

- รายการข้อกำหนดที่นำมาใช้ (SOA) จะเป็นเอกสารที่ระบุถึงวัตถุประสงค์ในการควบคุม (Control Objective) และมาตรการควบคุม (Controls) ด้านความมั่นคงปลอดภัย ที่บริษัท ไอรา พร็อพเพอร์ตี้ จำกัด (มหาชน) ได้เลือกนำมาใช้ในการดำเนินงานระบบ ISMS
- เอกสารดังกล่าวอย่างน้อยจะต้องประกอบไปด้วย
 - วัตถุประสงค์ในการควบคุม (Control Objective) และมาตรการ (Controls) ที่เลือกมาเพื่อจัดการความเสี่ยง
 - วัตถุประสงค์ในการควบคุม (Control Objective) และมาตรการ (Controls) ที่ใช้ในปัจจุบัน (Existing Control)
 - วัตถุประสงค์ในการควบคุม (Control Objective) และมาตรการ (Controls) ใน Annex A ที่ไม่เลือกนำมาใช้ในการจัดการความเสี่ยงและเหตุผลที่ไม่เลือก

3.2.3 จัดทำแผนการจัดการความเสี่ยงและนำไปใช้

- จัดทำแผนการจัดการความเสี่ยงตามผลที่ได้รับจากการประเมินความเสี่ยงและติดตามตรวจสอบการดำเนินงาน การประเมินความเสี่ยงคงเหลือในระบบ

3.2.4 การฝึกอบรมและการสร้างความเข้าใจเกี่ยวกับการดำเนินงานระบบ ISMS

- บุคลากรที่เกี่ยวข้องกับการดำเนินงานระบบ ISMS จะต้องได้รับการอบรม เกี่ยวกับการปฏิบัติตามกระบวนการต่างๆ ที่มีในระบบ
- บุคลากรควรได้รับการฝึกอบรม 2 ประเภท (ตามความเหมาะสม) ดังนี้
 - การอบรมทั่วไป เพื่อให้เกิดความตระหนักเกี่ยวกับมาตรการที่บริษัท ไอรา พร็อพเพอร์ตี้ (มหาชน) นำมาใช้รวมถึงระดับชั้นความลับและกระบวนการในการจัดการข้อมูล
 - การฝึกอบรมเฉพาะทางเพื่อช่วยเพิ่มความชำนาญในการปฏิบัติงาน

3.2.5 การบริหารการดำเนินการ

- บันทึกและจัดเก็บเอกสารต่างๆ สามารถใช้เป็นหลักฐานเพื่อแสดงว่ามาตรการที่ได้นำมาใช้นั้นมีการนำไปใช้งานจริงและสอดคล้องกับข้อกำหนด

- บันทึกดังกล่าวจะต้องได้รับการควบคุมตามระเบียบการปฏิบัติ เรื่องขั้นตอนการควบคุมเอกสาร และบันทึกการใช้งาน (Record Control Procedure)

3.3 กิจกรรมตรวจสอบ (Check)

รายละเอียดของขั้นตอนตรวจสอบของกรอบวิธีดำเนินการระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ (ISMS Framework) มีดังนี้

3.3.1 การสรุปผลการดำเนินงานตาม

- คณะทำงานบริหารจัดการด้านความมั่นคงปลอดภัยสารสนเทศ ต้องตรวจสอบและสรุปผลการดำเนินงานด้านความมั่นคงปลอดภัยสารสนเทศ เพื่อรายงานแก่ฝ่ายบริหารโดยการสรุปผลตามข้อ (3.2) และหลักฐานหรือเหตุการณ์ต่าง ๆ ที่มีนัยสำคัญต่อประสิทธิภาพของระบบและการพัฒนาปรับปรุงอย่างต่อเนื่อง เช่น
 - ความคิดเห็นและผลตอบรับจากผู้ปฏิบัติงานในทุกระดับชั้น (Feedback)
 - ผลการประเมินความเสี่ยงและการบริหารจัดการความเสี่ยงตลอดจนความเสี่ยงคงเหลือในระบบ (Risk Management result)
 - ผลของการวัดประเมินประสิทธิภาพของระบบฯ (ISMS Measurement result)
 - เหตุการณ์สำคัญที่มีผลกระทบต่อระบบฯ (Event)
 - โอกาสในการพัฒนาปรับปรุงอย่างต่อเนื่อง (Opportunity for improvement)

3.3.2 การตรวจประเมินภายใน (Internal Audit)

คณะตรวจประเมินภายในดำเนินการตรวจสอบความสอดคล้อง ดังต่อไปนี้

- ความสอดคล้องต่อนโยบายของบริษัท ไอรา พร็อพเพอร์ตี้ จำกัด (มหาชน)
- ความสอดคล้องต่อข้อกำหนดของมาตรฐานสากล ISO/IEC 27001: 2022
- ความสอดคล้องด้านกฎหมายและข้อบังคับทางสัญญาจากหน่วยงานที่เกี่ยวข้องกับระบบฯ
- ผลการตรวจสอบจะต้องถูกนำเสนอฝ่ายบริหารเพื่อพิจารณา

3.3.3 การวัดผลประสิทธิภาพระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ

- วัดผลและทบทวนประสิทธิภาพการดำเนินงานโดยตัวชี้วัด
- ตัวชี้วัดดังกล่าวจะใช้ในการหาสาเหตุของการขาดประสิทธิภาพในระบบการบริหารจัดการและการดำเนินงานตามมาตรฐานข้อกำหนดรวมทั้งประเด็นต่างๆที่จะต้องดำเนินการแก้ไขและปรับปรุง

3.3.4 การประชุมทบทวนของผู้บริหาร

- การทบทวนการดำเนินงานระบบ ISMS โดยฝ่ายบริหารจะต้องจัดขึ้นอย่างน้อย 1 ครั้งต่อปี โดยผลของการทบทวนต้องมีการจัดเก็บเป็นลายลักษณ์อักษรและแสดงถึง
- ผลการตรวจประเมินภายในและการแก้ไขผลการประเมิน ความเสี่ยงและการจัดการความเสี่ยง
- ความคิดเห็น (Feedback) จากผู้ปฏิบัติงานและผู้ที่เกี่ยวข้อง
- การเปลี่ยนแปลงปัจจัยภายในภายนอกที่ส่งผลกระทบต่อประสิทธิภาพของระบบ
- บริหารจัดการความมั่นคงปลอดภัยสารสนเทศ

- ผลการวัดประสิทธิภาพของระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ เหตุการณ์หรือการละเมิดความมั่นคงปลอดภัยสารสนเทศที่เกิดขึ้น (Incident)
- ผลจากการทำ Management review ที่ผ่านมาและการแก้ไขตามคำแนะนำของฝ่ายบริหาร
- โอกาสในการปรับปรุงระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ

3.4 กิจกรรมปรับปรุง (Act)

รายละเอียดของขั้นตอนการปรับปรุงวิธีดำเนินการระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ (ISMS Framework) มีดังนี้

3.4.1 การแก้ไขข้อบกพร่อง

- ปัญหาหรือความไม่สอดคล้องต่างๆ ต้องได้รับการแก้ไขและติดตามผลผ่านกระบวนการทำ Corrective Action

3.4.2 การพัฒนาปรับปรุงอย่างต่อเนื่อง

- บริษัท ไอรา พร็อพเพอร์ตี้ จำกัด (มหาชน) ต้องดำเนินกิจกรรมการพัฒนาปรับปรุงระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศตามแนวทางที่ได้มีการกำหนดขึ้นอย่างต่อเนื่อง

3.5 การสนับสนุน (Support)

กิจกรรมสนับสนุนถือว่ามีความซับซ้อนเพิ่มเติมในวงจร P-D-C-A เพราะเป็นกิจกรรมที่เกิดขึ้น ตลอดการดำเนินกิจกรรมในระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ เช่น

3.5.1 การควบคุมเอกสารและหลักฐานการดำเนินการกิจกรรม

- บริษัท ไอรา พร็อพเพอร์ตี้ จำกัด (มหาชน) ต้องควบคุมหลักฐานการดำเนินการกิจกรรมเพื่อใช้ยืนยันความสอดคล้องและแนวทางการปฏิบัติงานตามกระบวนการควบคุมเอกสารที่ได้มีการจัดทำขึ้นและสอดคล้องกับข้อกำหนดของมาตรฐานและหมายรวมถึงการควบคุมเอกสารภายนอกที่เกี่ยวข้อง
- หลักฐานและเอกสารในทุกรูปแบบต้องมีการจัดเก็บและควบคุมตามระดับชั้นความลับ และระยะเวลาการจัดเก็บที่เหมาะสม

บริษัท ไอรา พร็อพเพอร์ตี้ จำกัด (มหาชน) ต้องพิจารณาโอกาสในการส่งเสริมศักยภาพของบุคลากร ความพร้อมทางด้านทักษะในการดำเนินกิจกรรมให้บรรลุวัตถุประสงค์และความคาดหวังในหน้าที่ความรับผิดชอบ

ประกาศ ณ วันที่ 7 พฤศจิกายน 2568