บริษัท เจ เอ็ม ที เน็ทเวอร์ค เซอร์วิสเซ็ส จำกัด (มหาชน)

นโยบายระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ
(Information Security Management System Policy)
ISMS-1PC-001

ระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ

Information Security Management System (ISMS)

ISO/IEC 27001: 2013

รหัสเอกสาร:	ISMS-1PC-001 [Information Security Management System Policy]
ชื่อเอกสาร:	นโยบายระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ
หมายเลขปรับปรุงเอกสาร:	2565-V1.0
วันที่เอกสารมีผลบังคับใช้:	1/8/65
เจ้าของเอกสาร:	ฝ่ายเทคโนโลยีสารสนเทศ

ลายเซ็นรับรองเอกสาร

หน้าที่	ชื่อ		ตำแหน่ง	ลายเซ็น	วันที่
จัดทำโดย	วิริยศิษฐ์	มีสวัสดิ์	IT manager	วิริยศิษฐ์	1/8/65
ทบทวน	ชินวัฒน์	มังกรเดชสกุล	ISMR		1/8/65
อนุมัติ	ณัชชา	ฉินศิศโสภณ	ประธานคณะกรรมการ ISMS		1/8/65

ประวัติการปรับปรุงเอกสาร

หมายเลขปรับปรุงเอกสาร (version):	คำอธิบายและเหตุผลในการแก้ไข
1.0	เอกสารเผยแพร่ฉบับแรก

สารบัญ

1. วัตถุประสงค์ 4
2. นโยบายสำหรับระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ 4
   - 2.1 ข้อกำหนดด้านความมั่นคงปลอดภัยสารสนเทศ 4
   - 2.2 หลักการด้านความมั่นคงปลอดภัยสารสนเทศ 5
   - 2.3 เป้าหมายของความมั่นคงปลอดภัยสารสนเทศ 5
   - 2.4 การจัดทำกลยุทธ์ด้านความมั่นคงปลอดภัยสารสนเทศ 6
   - 2.5 การกำกับดูแลและหน้าที่ความรับผิดชอบ 7
3. กรอบการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ 11
   - 3.1 กิจกรรมวางแผน (Plan) 11
   - 3.2 กิจกรรมดำเนินการ (Do) 13
   - 3.3 กิจกรรมตรวจสอบ (Check) 15
   - 3.4 กิจกรรมปรับปรุง (Act) 17
   - 3.5 การสนับสนุน (Support) 18

1. วัตถุประสงค์

นโยบายฉบับนี้ จัดทำขึ้นเพื่อเป็นแนวทางหลักในการดำเนินกิจกรรมในระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศของบริษัท เจ เอ็ม ที เน็ทเวอร์ค เซอร์วิสเซ็ส จำกัด (มหาชน) โดยการกำหนดนโยบายระดับสูง หน้าที่ความรับผิดชอบที่จำเป็นในการดำเนินกิจกรรม และรายการกิจกรรมในระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ

2. นโยบายสำหรับระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ

2.1 ข้อกำหนดด้านความมั่นคงปลอดภัยสารสนเทศ

ในการดำเนินงานบนระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศนั้น จะต้องเป็นไปตามข้อกำหนดด้านความมั่นคงปลอดภัยในแต่ละด้าน ดังต่อไปนี้

<u>ข้อกำหนดตามการกำหนดค่าเป้าหมายและการรายงานผลการปฏิบัติงานตามตัวชี้วัด (KPI)</u>

ระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ จำเป็นต้องวัดผลประสิทธิภาพได้ โดยใช้ตัวชี้วัดที่มีความสอดคล้องกับนโยบายหน่วยงาน ความเสี่ยง ตลอดจนการวัดประสิทธิภาพของมาตรการควบคุมเชิงความปลอดภัยสารสนเทศที่บริษัท เจ เอ็ม ที เน็ทเวอร์ค เซอร์วิสเซ็ส จำกัด (มหาชน) ได้นำมาใช้ ทั้งนี้ ผลประสิทธิภาพต้องได้รับการรายงานแก่คณะผู้บริหารและสื่อสารไปถึงทุกหน่วยงานที่เกี่ยวข้อง โดยกำหนดให้การวัดผลประสิทธิภาพของระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศต้องทำขึ้น<u>อย่างน้อย 1 ครั้งต่อปี</u> โดยตัวชี้วัดต้องครอบคลุมทุกหน่วยงานภายใต้ขอบเขตการดำเนินงาน

<u>ข้อกำหนดเชิงกฎหมาย</u>

ระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ จำเป็นต้องมีความสอดคล้องตามข้อกำหนดกฎหมาย กฎระเบียบบังคับ ตลอดจนนโยบายทั้งภายในและภายนอกบริษัท เจ เอ็ม ที เน็ทเวอร์ค เซอร์วิสเซ็ส จำกัด (มหาชน) ที่มีส่วนเกี่ยวข้องทั้งโดยตรงและโดยอ้อมในการดำเนินกิจกรรม โดยเป็นหน้าที่สำคัญของบุคลากรทุกคนภายใต้ขอบเขตการดำเนินงานที่ต้องศึกษาทำความเข้าใจกับข้อกำหนดต่างๆ

ทั้งนี้ รายการข้อกฎหมายที่เกี่ยวข้องกับระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ ได้แก่

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

อ้างอิง: เอกสารรายการประเมินความสอดคล้องข้อกฎหมาย (Legal)

ข้อกำหนดตามมาตรฐานสากล ISO/IEC 27001: 2013

ระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ ต้องมีความสอดคล้องกับข้อกำหนดตามมาตรฐานสากล ISO/IEC 27001: 2013 ทั้งในส่วนของระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ และรายการมาตรการควบคุมที่นำมาใช้

อ้างอิง: เอกสารรายการมาตรการด้านความมั่นคงปลอดภัยสารสนเทศที่นำมาประยุกต์ใช้ (Statement of Applicability)

2.2 หลักการด้านความมั่นคงปลอดภัยสารสนเทศ

ระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ ใช้แนวทางด้านความมั่นคงปลอดภัยของสารสนเทศโดยพิจารณาองค์ประกอบ 3 ข้อหลัก ได้แก่

องค์ประกอบ	คำอธิบาย
ความลับ (Confidentiality)	การรักษาไว้ซึ่งความลับของสารสนเทศ ไม่ถูกเปิดเผยแก่ระบบ คน และ/หรือ หน่วยงานที่ไม่ได้มีส่วนเกี่ยวข้อง
ความสมบูรณ์ (Integrity)	การรักษาไว้ซึ่งความถูกต้องเสถียรภาพของสารสนเทศ ไม่ถูกแก้ไขหรือนำไปใช้อย่างผิดวิธี และสามารถตรวจสอบความถูกต้องของสารสนเทศก่อนการนำไปใช้งานได้
ความพร้อมใช้ (Availability)	การรักษาไว้ซึ่งความพร้อมใช้งานของสารสนเทศ

โดยองค์ประกอบข้างต้น จะถูกนำมาพิจารณาเป็นมูลค่าของทรัพย์สินสารสนเทศในเชิงความมั่นคงปลอดภัย อันรวมไปถึงทรัพย์สินอื่นๆ ที่เกี่ยวข้องกับสารสนเทศ

ความมั่นคงปลอดภัยสารสนเทศบนพื้นฐานของความเสี่ยง (Information Security aspects to risk based approach)

ระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ ยึดแนวทางการพิจารณาความเสี่ยงที่มีผลกระทบต่อทรัพย์สินสารสนเทศทั้งทางตรงและทางอ้อม ผ่านการประเมินมูลค่าความเสียหายและโอกาสการเกิดขึ้นของภัยคุกคามที่อาศัยช่องโหว่ของทรัพย์สินหรือระบบฯ ที่ไม่มีประสิทธิภาพ

อ้างอิง: เอกสารระเบียบขั้นตอนการบริหารจัดการความเสี่ยง (Risk Management Methodology)

2.3 เป้าหมายของความมั่นคงปลอดภัยสารสนเทศ

เป้าหมายสำคัญของการดำเนินกิจกรรมตามระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ คือ การลดและหลีกเลี่ยงปัญหาการละเมิดความมั่นคงปลอดภัยสารสนเทศ อันส่งผลต่อภาพลักษณ์และความเชื่อมั่นของผู้ใช้บริการ Data Center คือ การพัฒนาระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศภายใน Data Center

เพื่อให้ได้รับรองมาตรฐานสากลด้านความมั่นคงปลอดภัยสารสนเทศอย่างต่อเนื่อง และการเป็นมืออาชีพในการให้บริการด้วยระบบเทคโนโลยีสารสนเทศที่มีความมั่นคงปลอดภัย (Information Security)

2.4 การจัดทำกลยุทธ์ด้านความมั่นคงปลอดภัยสารสนเทศ

กลยุทธ์ด้านความมั่นคงปลอดภัยมีการกำหนดขึ้น เพื่อสร้างกรอบการปฏิบัติแก่ผู้ปฏิบัติงานภายใต้ขอบเขต โดยการเข้าใจถึงวัตถุประสงค์และแนวทางที่สามารถใช้ในการดำเนินกิจกรรม โดยมีการกำหนดกลยุทธ์ดังต่อไปนี้

<u>ความสามารถในการปรับเปลี่ยนเพื่อสร้างความสอดคล้อง (Flexibility)</u>

ระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ ควรถูกออกแบบให้มีความเหมาะสมกับสภาวะแวดล้อมของบริษัท เจ เอ็ม ที เน็ทเวอร์ค เซอร์วิสเซ็ส จำกัด (มหาชน) สามารถเปลี่ยนแปลงตามปัจจัยต่างๆ เพื่อให้ผู้ปฏิบัติงานสามารถนำระบบฯ ไปใช้งานได้จริงไม่ก่อให้เกิดความยากลำบากในการดำเนินงาน หรือใช้เวลามากจนเกินพอดี

<u>ระบบบริหารจัดการความมั่นคงปลอดภัยบนพื้นฐานของความเสี่ยง (Risk based approach)</u>

บริษัท เจ เอ็ม ที เน็ทเวอร์ค เซอร์วิสเซ็ส จำกัด (มหาชน) ต้องพิจารณาถึงความเสี่ยงด้านข้อมูลสารสนเทศเป็นสำคัญ เพื่อพิจารณาถึงการเลือกใช้มาตรการควบคุมหรือการกำหนดนโยบายต่างๆ ให้เกิดความสอดคล้อง โดยให้มุ่งเน้นถึงผลกระทบในทุกด้านที่เกี่ยวข้อง และระดับการควบคุมป้องกันภัยคุกคามที่เหมาะสม

<u>การส่งเสริมศักยภาพบุคลากร และทักษะที่จำเป็นในการรับมือความมั่นคงปลอดภัยสารสนเทศ</u>

บริษัท เจ เอ็ม ที เน็ทเวอร์ค เซอร์วิสเซ็ส จำกัด (มหาชน) ต้องมั่นใจว่าบุคลากรภายใต้ขอบเขตระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ มีทักษะความสามารถเพียงพอต่อการทำกิจกรรมต่างๆ โดยทักษะความสามารถแบ่งออกเป็น

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

2.5 การกำกับดูแลและหน้าที่ความรับผิดชอบ

<u>คณะกรรมการบริหารความมั่นคงปลอดภัยสารสนเทศ (ISMS Committee)</u>

คณะกรรมการบริหารความมั่นคงปลอดภัยสารสนเทศ (ISMS Committee) มีหน้าที่ในการวางแผน จัดการ สนับสนุนให้ทุกกิจกรรมที่เกี่ยวข้องกับความมั่นคงปลอดภัยสารสนเทศเป็นไปตามข้อกำหนดในนโยบาย ทั้งนี้ คณะกรรมการบริหารความมั่นคงปลอดภัยสารสนเทศ (ISMS Committee) ต้องดำเนินการดังต่อไปนี้

- ตรวจทานและอนุมัติกรอบการดำเนินงานและนโยบายด้านความมั่นคงปลอดภัยสารสนเทศ
- กำหนดทิศทางและให้คำปรึกษาในการสร้าง รวมถึงพัฒนาระบบการรักษาความมั่นคงปลอดภัยสารสนเทศ
- กำหนดเป้าหมายและวัตถุประสงค์ของการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ
- สนับสนุนทรัพยากรที่จำเป็น เพื่อให้บรรลุวัตถุประสงค์ด้านความมั่นคงปลอดภัยสารสนเทศที่หน่วยงานกำหนดไว้
- พิจารณาและอนุมัติวิธีการบริหารจัดการความเสี่ยง (Risk Management Methodology) และระดับความเสี่ยงที่หน่วยงานยอมรับได้ (Acceptable Risk Level หรือ ARL)
- พิจารณาแผนการดำเนินการจัดการความเสี่ยงและความเสี่ยงที่เหลืออยู่ รวมถึงอนุมัติกรอบการบริหารจัดการความต่อเนื่องของธุรกิจ ให้สอดคล้องกับเป้าหมายของหน่วยงาน
- ให้คำปรึกษาในการดำเนินงานระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ (ISMS) ตามมาตรฐาน ISO/IEC 27001: 2013
- ปรับปรุงข้อกำหนด ข้อกฎหมายที่เกี่ยวข้องกับขอบเขตระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ (ISMS Scope) ให้มีความเหมาะสม
- ดำรงตำแหน่งเป็นเจ้าของความเสี่ยง (Risk Owner) มีอำนาจในการพิจารณาการอนุมัติแผนการจัดการความเสี่ยง ผลการประเมิน ตลอดจนแนวทางมาตรการที่เหมาะสม ทั้งนี้ ผู้บริหารสามารถมอบหมายหน้าที่ความรับผิดชอบในการดูแลความเสี่ยงให้แก่ ISMR หรือผู้ที่ได้รับการแต่งตั้งได้
- ทบทวนการบริหารจัดการระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ (ISMS Management Review)
- ทบทวนและอนุมัติ กรณีนโยบายและมาตรฐานที่มีอยู่ไม่ครอบคลุมความเสี่ยงดังกล่าว
- อนุมัติความเสี่ยงคงเหลือ (Residual Risk) ในระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ

- มีอำนาจแต่งตั้งคณะทำงานบริหารจัดการด้านความมั่นคงปลอดภัยสารสนเทศ (ISMS Working Team) เจ้าหน้าที่ดูแลเอกสาร (Document Control Officer) และ คณะผู้ตรวจสอบภายในระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ (ISMS Internal Audit)
- ปฏิบัติหน้าที่อื่นๆ ตามที่ประธานกรรมการบริหารของ บริษัทฯ มอบหมาย

<u>ผู้บริหารจัดการด้านความมั่นคงปลอดภัยสารสนเทศ (ISMS Management Representative: ISMR)</u>

ผู้บริหารจัดการด้านความมั่นคงปลอดภัยสารสนเทศ (ISMR) มีหน้าที่รายงานผลการดำเนินการต่อคณะกรรมการบริหารความมั่นคงปลอดภัยสารสนเทศ (ISMS Committee) โดยมีความรับผิดชอบดังต่อไปนี้

- ควบคุมและแก้ไขปัญหาให้การบริหารจัดการความมั่นคงปลอดภัยข้อมูลสารสนเทศ ถูกนำไปใช้ได้อย่างมีประสิทธิภาพ
- รายงานประสิทธิภาพการดำเนินงานของระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ (ISMS) ต่อคณะกรรมการ ISMS Committee ในขั้นตอนการทบทวนของฝ่ายบริหาร หรือ Management Review Meeting
- ดำเนินการร่วมกับคณะตรวจประเมินภายใน ในการติดต่อกับหน่วยงานที่ให้การรับรอง เพื่อวางแผนและกำหนดแผนในการตรวจประเมินระบบ ISMS ตามมาตรฐาน ISO/IEC 27001: 2013
- ติดตามการดำเนินการและการปฏิบัติงานของระบบ ISMS ในการใช้งานจริงและประสานกับผู้ที่เกี่ยวข้องในการเฝ้าระวัง รักษา ทบทวนและปรับปรุงระบบ ISMS
- ตรวจสอบผลการดำเนินการ รวมถึงดำเนินงานร่วมกับคณะทำงาน ISMS เพื่อประเมินประสิทธิภาพและความสอดคล้องของระบบ ISMS
- รับผิดชอบในการนำระบบ ISMS ไปใช้งานจริงและดูแลให้การนำไปใช้งานเป็นไปตามวัตถุประสงค์ของการจัดทำระบบ ISMS
- ดำรงตำแหน่งเป็นเจ้าของความเสี่ยง (Risk Owner) เมื่อได้รับการแต่งตั้งหรือมอบหมายจากคณะผู้บริหาร
- ปฏิบัติหน้าที่อื่นๆ ตามที่คณะบริหารความมั่นคงปลอดภัยสารสนเทศมอบหมาย

<u>คณะทำงานบริหารจัดการด้านความมั่นคงปลอดภัยสารสนเทศ (ISMS Working Team)</u>

คณะทำงาน ISMS คือผู้ประสานงานผู้บริหารจัดการด้านความมั่นคงปลอดภัยสารสนเทศ (ISMR) โดยให้คำแนะนำการดำเนินงานที่เกี่ยวข้องกับความมั่นคงปลอดภัยสารสนเทศในบริษัท เจ เอ็ม ที เน็ทเวอร์ค เซอร์วิสเซ็ส จำกัด (มหาชน) ซึ่งมีความรับผิดชอบดังต่อไปนี้

- เป็นผู้แทนหน่วยงานในการร่วมมือและนำระบบ ISMS ไปปฏิบัติในหน่วยงานของตน

- ดำเนินการตามนโยบายด้านการบริหารจัดการความมั่นคงปลอดภัยข้อมูลสารสนเทศ
- อบรมและสร้างความตระหนักด้านการรักษาความมั่นคงปลอดภัยสารสนเทศให้แก่พนักงานในหน่วยงาน
- ดำเนินการประเมินความเสี่ยงตามกระบวนการที่หน่วยงานกำหนดไว้
- รายงานการดำเนินงานต่อผู้แทนกรรมการบริหารจัดการความมั่นคงปลอดภัยข้อมูลสารสนเทศ (ISMR) และนำระบบ ISMS มาปฏิบัติใช้
- สนับสนุนและดูแลให้มีการนำนโยบายด้านความมั่นคงปลอดภัยมาใช้อย่างเหมาะสม
- ตรวจสอบและปรับปรุงแก้ไขกระบวนการอย่างสม่ำเสมอให้มีความเหมาะสมและมีประสิทธิภาพ
- ให้คำแนะนำและชี้แจง เพื่อให้พนักงานและบุคคลที่เกี่ยวข้องปฏิบัติตามข้อกำหนด และเป็นไปตามมาตรฐาน ISO/IEC 27001: 2013 รวมถึงข้อกฎหมายและข้อบังคับที่เกี่ยวข้อง
- ดำเนินการจัดทำ ติดตามและปรับปรุงแผนการสื่อสารของระบบ ISMS
- ดำเนินการจัดทำ ติดตามและตรวจสอบผลการดำเนินการตามตัวชี้วัดประสิทธิภาพของระบบ ISMS
- ร่วมกิจกรรมการประเมินความเสี่ยงของทรัพย์สินสารสนเทศของหน่วยงานที่เกี่ยวข้อง
- ติดตามและตรวจสอบการเปลี่ยนแปลงของภัยคุกคามที่สำคัญ ที่เกี่ยวข้องกับทรัพย์สินสารสนเทศที่มีความเสี่ยง
- รายงานและวิเคราะห์เหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัยสารสนเทศ พร้อมดำเนินการแก้ไขและป้องกันการเกิดซ้ำ
- แก้ไขและกำหนดวิธีการป้องกัน เพื่อให้ระบบ ISMS ดำเนินการไปตามนโยบายที่องค์กรกำหนดไว้
- ชี้แจงและให้ความรู้แก่บุคลากร ผู้ใช้บริการ หน่วยงานพันธมิตร ตลอดจนผู้จัดจำหน่ายและบำรุงรักษา (Vendor) ที่เกี่ยวข้องให้สามารถปฏิบัติตามข้อกำหนด นโยบาย ข้อกฎหมาย และข้อบังคับอื่นๆ ที่เกี่ยวข้องได้อย่างถูกต้อง
- ประสานงานระหว่างคณะกรรมการและหน่วยงานอื่นที่เกี่ยวข้อง เพื่อดำเนินการให้ได้ตามที่กำหนดไว้ในระบบ ISMS
- ปฏิบัติหน้าที่อื่นๆ ตามที่คณะบริหารความมั่นคงปลอดภัยสารสนเทศมอบหมาย

คณะตรวจประเมินภายใน (Internal Auditor)

คณะตรวจประเมินภายใน จะเป็นผู้ตรวจสอบผลการดำเนินงานด้านการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ ตลอดจนกระบวนการต่างๆ เพื่อให้มั่นใจว่าสอดคล้องกับนโยบายด้านความมั่นคงปลอดภัยสารสนเทศและมาตรฐานข้อกำหนดที่เกี่ยวข้อง โดยมีหน้าที่ความรับผิดชอบดังนี้

- จัดเตรียมแผนการตรวจประเมิน
- จัดให้มีกิจกรรมการตรวจประเมินตามแผนที่กำหนดไว้
- จัดอบรมผู้ตรวจประเมินให้มีความรู้ความสามารถในการปฏิบัติงานได้อย่างเหมาะสม
- ดำเนินการตรวจประเมินและจัดทำรายงานผลการตรวจประเมิน
- ติดตามและตรวจสอบผลการแก้ไขและการป้องกัน
- รายงานผลการตรวจประเมินภายในของระบบ ISMS ต่อคณะกรรมการ ISMS Committee
- ดำเนินการร่วมกับ ISMR ในการติดต่อกับหน่วยงานที่ให้การรับรอง เพื่อวางแผนและกำหนดแผนในการตรวจประเมินระบบ ISMS ตามมาตรฐาน ISO/IEC 27001: 2013

เจ้าของระบบ (System Owner)

เจ้าของระบบ คือ บุคคลซึ่งได้รับมอบหมายให้จัดการข้อมูลสารสนเทศในระบบงานของตนเอง โดยเจ้าของระบบสารสนเทศจะต้องเป็นผู้ร่วมกำหนดนโยบายสนับสนุนด้านความมั่นคงปลอดภัยระบบสารสนเทศของการให้บริการ ตลอดจนตรวจทานและรับรองสิทธิการเข้าใช้ระบบงานตามขอบเขตที่รับผิดชอบให้เหมาะสมกับระดับชั้นความลับของข้อมูล

ผู้ดูแลระบบ (Custodian)

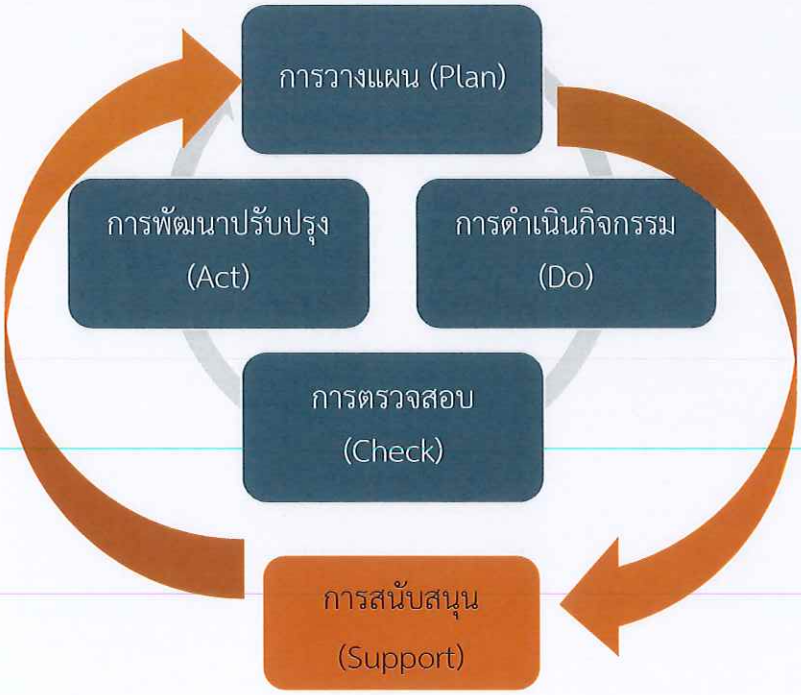
ผู้ดูแลระบบ คือ บุคคลซึ่งได้รับมอบหมายให้บริหารจัดการระบบสารสนเทศจากเจ้าของระบบ (System Owner) โดยจะต้องปฏิบัติตามนโยบายด้านความมั่นคงปลอดภัยระบบสารสนเทศของการให้บริการ ข้อตกลงร่วมของระดับการให้บริการ (Service Level Agreement) และขั้นตอนการปฏิบัติงานด้านการรักษาความมั่นคงปลอดภัยที่เจ้าของบริการกำหนดไว้ และดูแลให้ระบบสารสนเทศดังกล่าวสามารถให้บริการได้สอดคล้องกับข้อกำหนดในนโยบายด้านความมั่นคงปลอดภัยด้วย ทั้งนี้ การเพิ่มหรือเพิกถอนสิทธิในการเข้าถึงระบบใดๆ ให้ปฏิบัติตามเอกสารกระบวนการที่เจ้าของบริการกำหนดอย่างเคร่งครัด ตลอดจนทบทวนความเหมาะสมของมาตรการที่นำมาใช้ พร้อมทั้งรายงานผลการดำเนินงานให้เจ้าของระบบ (System Owner) ทราบเป็นระยะ

<u>ผู้ใช้ (User)</u>

ผู้ใช้ ได้แก่ บุคคล (หรือบางครั้งอาจหมายถึงระบบสารสนเทศหรือกระบวนการ) ที่ได้รับอนุญาตให้สามารถเข้าถึงข้อมูลสารสนเทศได้ตามกระบวนการหรือข้อบังคับของเจ้าของระบบเอง อย่างไรก็ตามผู้ใช้จะต้องปกป้องข้อมูลภายใต้การควบคุมของผู้ดูแลระบบ และจะต้องปฏิบัติตามข้อกำหนดในนโยบาย มาตรฐาน และแนวทางการดำเนินงานที่เกี่ยวข้อง ทั้งนี้ ผู้ใช้จะต้องรับผิดชอบการดำเนินการใดๆ ที่เกี่ยวข้องกับการใช้งานข้อมูลสารสนเทศ หากทราบหรือสงสัยว่ามีการละเมิดนโยบายความมั่นคงปลอดภัยสารสนเทศ จะต้องรายงานต่อผู้บังคับบัญชาหรือผู้บริหารจัดการด้านความมั่นคงปลอดภัยสารสนเทศ (ISMR) โดยทันที

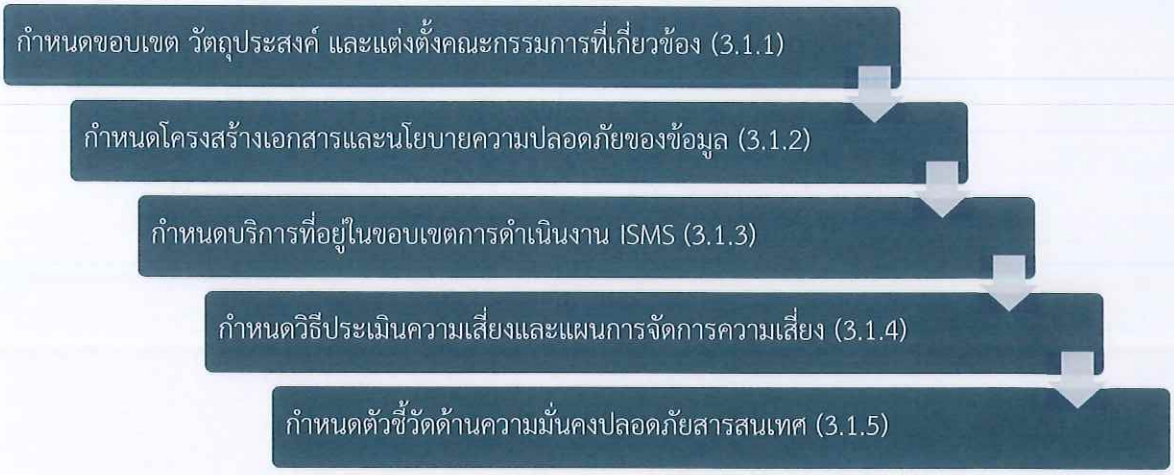
3. กรอบการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ

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



3.1 กิจกรรมวางแผน (Plan)

รายละเอียดของกิจกรรมนี้ ประกอบไปด้วยกระบวนการ 5 ขั้นตอน ดังนี้



<u>กำหนดขอบเขต วัตถุประสงค์ และแต่งตั้งคณะกรรมการที่เกี่ยวข้อง (3.1.1)</u>

- การกำหนดขอบเขตของการนำระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ (ISMS) รวมถึงการกำหนดพันธกิจ วิสัยทัศน์ ตลอดจนวัตถุประสงค์ทางด้านความปลอดภัยสารสนเทศ ให้สอดคล้องกับเป้าหมายและวัตถุประสงค์ของบริษัท เจ เอ็ม ที เน็ทเวอร์ค เซอร์วิสเซ็ส จำกัด (มหาชน)
- การกำหนดปัจจัยและปัญหาที่นำมาสู่การดำเนินกิจกรรมในระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศของบริษัท เจ เอ็ม ที เน็ทเวอร์ค เซอร์วิสเซ็ส จำกัด (มหาชน) ตลอดจนผู้ที่เกี่ยวข้องและความไม่เป็นอิสระต่อหน่วยงานต่างๆ
- แต่งตั้งคณะกรรมการทางด้าน ISMS เพื่อร่วมขับเคลื่อนระบบ ISMS ภายใต้ขอบเขตที่กำหนดไว้
- จัดทำเอกสารนโยบายระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ ซึ่งจะกำหนดพันธกิจ วิสัยทัศน์ วัตถุประสงค์ ตลอดจนหน้าที่ความรับผิดชอบของคณะกรรมการที่เกี่ยวข้องกับการดำเนินการระบบ ISMS และเอกสารขอบเขตระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ

<u>กำหนดโครงสร้างเอกสารและนโยบายความปลอดภัยของข้อมูล (3.1.2)</u>

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

<u>กำหนดขอบเขตการดำเนินงาน ISMS (3.1.3)</u>

- กำหนดบริการที่ต้องการจะรับการตรวจสอบเพื่อขอรับใบรับรอง (Certify) โดยต้องอยู่ในขอบเขตที่กำหนดไว้

- การกำหนดบริการและระบบสารสนเทศ รวมทั้งรายการทรัพย์สินสารสนเทศภายในขอบเขตของการดำเนินงาน จะพิจารณาตามประเด็นบริการด้านเทคโนโลยีสารสนเทศหลักที่มีผลต่อภารกิจของบริษัท เจ เอ็ม ที เน็ทเวอร์ค เซอร์วิสเซ็ส จำกัด (มหาชน)
- ข้อมูลดังกล่าวข้างต้น จะถูกจัดเก็บไว้ในรายการบัญชีทรัพย์สิน

<u>กำหนดวิธีประเมินความเสี่ยงและการจัดการความเสี่ยง (3.1.4)</u>

- วิธีที่ใช้ในการประเมินและการบริหารความเสี่ยงนั้น ได้นำกระบวนการควบคุมความเสี่ยงตามมาตรฐาน ISO/IEC 27005 หรือ ISO/IEC 31000 มาประยุกต์ใช้ โดยรายละเอียดของกระบวนการดังกล่าวจะอยู่ในเอกสารระเบียบขั้นตอนการบริหารจัดการความเสี่ยง (Risk Management Methodology)

<u>กำหนดตัวชี้วัด (3.1.5)</u>

- ต้องมีการกำหนดตัวชี้วัดเพื่อประเมินประสิทธิภาพของมาตรการต่างๆ ที่นำมาใช้
- ตัวชี้วัดจะต้องเป็นการวัดผลเชิงปริมาณ โดยตัวชี้วัดดังกล่าวจะต้องมีองค์ประกอบ ดังต่อไปนี้
  - ✓ เป้าหมายการนำไปใช้งาน (Objective of the metrics)
  - ✓ การวัดและวิเคราะห์ผล (Measurement of the metrics)
  - ✓ วัตถุประสงค์การนำไปใช้ (Purpose of metrics)
  - ✓ ความถี่ในการเก็บข้อมูล (Frequency)
  - ✓ การคำนวณค่าของตัวชี้วัด (Process Method)
- ต้องจัดทำเอกสารอ้างอิงเพื่อสนับสนุนการเก็บรวบรวมและวิเคราะห์ในเมตริกซ์ ตัวชี้วัดตัวเดียวกันอาจนำไปใช้สำหรับมาตรการอื่นๆ ได้ หากข้อมูลที่ได้จากตัวชี้วัดดังกล่าวสามารถนำไปใช้วัดผลวัตถุประสงค์ของมาตรการดังกล่าวได้

3.2 กิจกรรมดำเนินการ (Do)

รายละเอียดของขั้นตอนดำเนินการ (Do) ของกรอบวิธีดำเนินการระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ (ISMS Framework) เป็นดังต่อไปนี้

การประเมินความเสี่ยงและการจัดการความเสี่ยง (3.2.1)

จัดทำเอกสารรายการข้อกำหนดที่นำมาใช้ (statement of applicability) (3.2.2)

จัดทำแผนจัดการความเสี่ยงและนำไปใช้ (3.2.3)

การฝึกอบรมและการสร้างความเข้าใจเกี่ยวกับการดำเนินงานระบบ ISMS (3.2.4)

การบริหารการดำเนินการ (3.2.5)

<u>การประเมินความเสี่ยงและการจัดการความเสี่ยง (3.2.1)</u>

- ผู้ดูแลระบบและเจ้าของที่เกี่ยวข้องกับระบบสารสนเทศที่อยู่ในขอบเขตการดำเนินงานระบบ ISMS จะทำการตรวจสอบทรัพย์สินของตนเอง ประเมินผลกระทบ และความเสี่ยงของทรัพย์สินตามแนวทางการประเมินความเสี่ยง
- กำหนดระดับความเสี่ยงที่ยอมรับได้ (ARL) โดยเปรียบเทียบกับความเสี่ยงในปัจจุบัน และดำเนินการลดความเสี่ยงสำหรับทรัพย์สินที่มีค่าความเสี่ยงมากเกินกว่าค่าที่ยอมรับได้ (Overexposed Assets)

<u>จัดทำเอกสารรายการข้อกำหนดที่นำมาใช้ (Statement of Applicability) (3.2.2)</u>

- รายการข้อกำหนดที่นำมาใช้ (SOA) จะเป็นเอกสารที่ระบุถึงวัตถุประสงค์ในการควบคุม (Control Objective) และมาตรการควบคุม (Controls) ด้านความมั่นคงปลอดภัยที่บริษัท เจ เอ็ม ที เน็ทเวอร์ค เซอร์วิสเซ็ส 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

<u>จัดทำแผนการจัดการความเสี่ยงและนำไปใช้ (3.2.3)</u>

- จัดทำแผนการจัดการความเสี่ยงตามผลที่ได้รับจากการประเมินความเสี่ยง และติดตามตรวจสอบการดำเนินงาน การประเมินความเสี่ยงคงเหลือในระบบ

<u>การฝึกอบรมและการสร้างความเข้าใจเกี่ยวกับการดำเนินงานระบบ ISMS (3.2.4)</u>

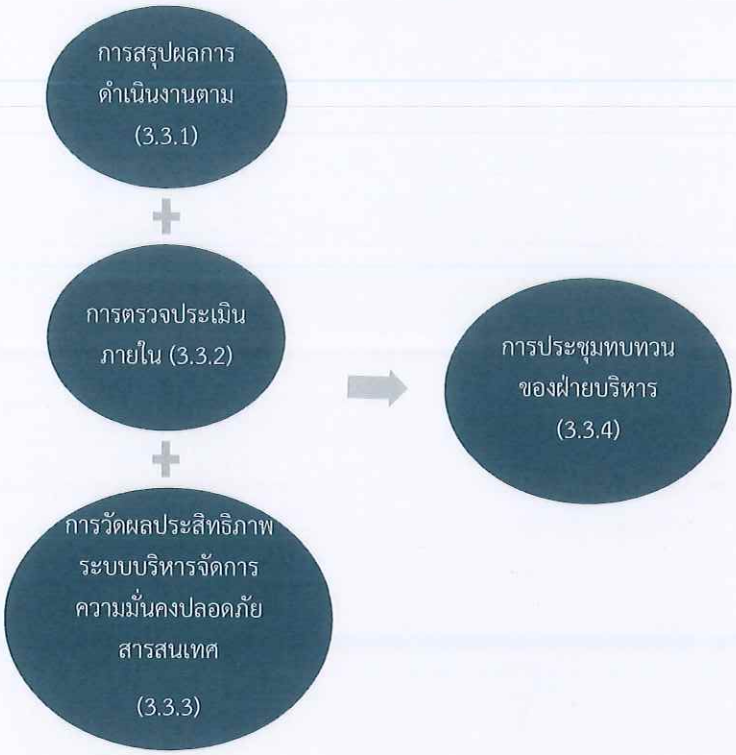
- บุคลากรที่เกี่ยวข้องกับการดำเนินงานระบบ ISMS จะต้องได้รับการอบรมเกี่ยวกับการปฏิบัติตามกระบวนการต่างๆ ที่มีในระบบ
- บุคลากรควรได้รับการฝึกอบรม 2 ประเภท (ตามความเหมาะสม) ดังนี้
  - ✓ การอบรมทั่วไป เพื่อให้เกิดความตระหนักเกี่ยวกับมาตรการที่บริษัท เจ เอ็ม ที เน็ทเวอร์ค เซอร์วิสเซ็ส จำกัด (มหาชน)นำมาใช้รวมถึงระดับชั้นความลับและกระบวนการในการจัดการข้อมูล
  - ✓ การฝึกอบรมเฉพาะทาง เพื่อช่วยเพิ่มความชำนาญในการปฏิบัติงาน

<u>การบริหารการดำเนินการ (3.2.5)</u>

- บันทึกและจัดเก็บเอกสารต่างๆ สามารถใช้เป็นหลักฐานเพื่อแสดงว่ามาตรการที่ได้นำมาใช้นั้น มีการนำไปใช้งานจริงและสอดคล้องกับข้อกำหนด
- บันทึกดังกล่าวจะต้องได้รับการควบคุมตามระเบียบการปฏิบัติ เรื่อง ขั้นตอนการควบคุมเอกสารและบันทึกการใช้งาน (Record Control Procedure)

3.3 กิจกรรมตรวจสอบ (Check)

รายละเอียดของขั้นตอนตรวจสอบของกรอบวิธีดำเนินการระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ (ISMS Framework) มีดังนี้



<u>การสรุปผลการดำเนินงานตาม (3.3.1)</u>

- คณะทำงานบริหารจัดการด้านความมั่นคงปลอดภัยสารสนเทศ ต้องตรวจสอบและสรุปผลการดำเนินงานด้านความมั่นคงปลอดภัยสารสนเทศ เพื่อรายงานแก่ฝ่ายบริหารโดยการสรุปผลตามข้อ (3.2) และหลักฐานหรือเหตุการณ์ต่างๆ ที่มีนัยสำคัญต่อประสิทธิภาพของระบบและการพัฒนาปรับปรุงอย่างต่อเนื่อง เช่น
  - ✓ ความคิดเห็นและผลตอบรับจากผู้ปฏิบัติงานในทุกระดับชั้น (Feedback)
  - ✓ ผลการประเมินความเสี่ยงและการบริหารจัดการความเสี่ยง ตลอดจนความเสี่ยงคงเหลือในระบบฯ (Risk Management result)
  - ✓ ผลของการวัดประเมินประสิทธิภาพของระบบฯ (ISMS Measurement result)
  - ✓ เหตุการณ์สำคัญที่มีผลกระทบต่อระบบฯ (Event)
  - ✓ โอกาสในการพัฒนาปรับปรุงอย่างต่อเนื่อง (Opportunity for improvement)

<u>การตรวจประเมินภายใน (Internal Audit) (3.3.2)</u>

- คณะตรวจประเมินภายใน ดำเนินการตรวจสอบความสอดคล้อง ดังต่อไปนี้
  - ✓ ความสอดคล้องต่อนโยบายของบริษัท เจ เอ็ม ที เน็ทเวอร์ค เซอร์วิสเซ็ส จำกัด (มหาชน)
  - ✓ ความสอดคล้องต่อข้อกำหนดของมาตรฐานสากล ISO/IEC 27001: 2013

- ✓ ความสอดคล้องด้านกฎหมายและข้อบังคับทางสัญญาจากหน่วยงานที่เกี่ยวข้องกับระบบฯ

- ผลการตรวจสอบจะต้องถูกนำส่งฝ่ายบริหารเพื่อพิจารณา

<u>การวัดผลประสิทธิภาพระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ (3.3.3)</u>

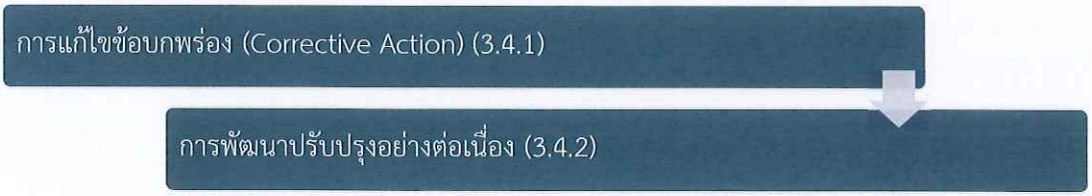
- วัดผลและทบทวนประสิทธิภาพการดำเนินงานโดยตัวชี้วัด
- ตัวชี้วัดดังกล่าวจะใช้ในการหาสาเหตุของการขาดประสิทธิภาพในระบบการบริหารจัดการ และการดำเนินงานตามมาตรฐานข้อกำหนด รวมทั้งประเด็นต่างๆ ที่จะต้องดำเนินการแก้ไขและปรับปรุง

<u>การประชุมทบทวนของผู้บริหาร (3.3.4)</u>

- การทบทวนการดำเนินงานระบบ ISMS โดยฝ่ายบริหารจะต้องจัดขึ้น<u>อย่างน้อย 1 ครั้งต่อปี</u> โดยผลของการทบทวนต้องมีการจัดเก็บเป็นลายลักษณ์อักษรและแสดงถึง
  - ✓ ผลการตรวจประเมินภายในและการแก้ไข
  - ✓ ผลการประเมินความเสี่ยงและการจัดการความเสี่ยง
  - ✓ ความคิดเห็น (Feedback) จากผู้ปฏิบัติงานและผู้ที่เกี่ยวข้อง
  - ✓ การเปลี่ยนแปลงปัจจัยภายในภายนอกที่ส่งผลกระทบต่อประสิทธิภาพของระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ
  - ✓ ผลการวัดประสิทธิภาพของระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ
  - ✓ เหตุการณ์หรือการละเมิดความมั่นคงปลอดภัยสารสนเทศที่เกิดขึ้น (Incident)
  - ✓ ผลจากการทำ Management review ที่ผ่านมาและการแก้ไขตามคำแนะนำของฝ่ายบริหาร
  - ✓ โอกาสในการปรับปรุงระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ

3.4 กิจกรรมปรับปรุง (Act)

รายละเอียดของขั้นตอนการปรับปรุงวิธีดำเนินการระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ (ISMS Framework) มีดังนี้



การแก้ไขข้อบกพร่อง (3.4.1)

- ปัญหาหรือความไม่สอดคล้องต่างๆ ต้องได้รับการแก้ไขและติดตามผลผ่านกระบวนการทำ Corrective Action

การพัฒนาปรับปรุงอย่างต่อเนื่อง (3.4.2)

- บริษัท เจ เอ็ม ที เน็ทเวอร์ค เซอร์วิสเซ็ส จำกัด (มหาชน) ต้องดำเนินกิจกรรมการพัฒนาปรับปรุงระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ ตามแนวทางที่ได้มีการกำหนดขึ้นอย่างต่อเนื่อง

3.5 การสนับสนุน (Support)

กิจกรรมสนับสนุนถือว่ามีบทบาทเพิ่มเติมในวงจร P-D-C-A เพราะเป็นกิจกรรมที่เกิดขึ้นตลอดการดำเนินกิจกรรมในระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ เช่น

การควบคุมเอกสารและหลักฐานการดำเนินกิจกรรม (3.5.1)

- บริษัท เจ เอ็ม ที เน็ทเวอร์ค เซอร์วิสเซ็ส จำกัด (มหาชน) ต้องควบคุมหลักฐานการดำเนินกิจกรรมเพื่อใช้ยืนยันความสอดคล้องและแนวทางการปฏิบัติที่ดีงาม ตามกระบวนการควบคุมเอกสารที่ได้มีการจัดทำขึ้น และสอดคล้องกับข้อกำหนดของมาตรฐาน และหมายรวมถึงการควบคุมเอกสารภายนอกที่เกี่ยวข้อง
- หลักฐาน และเอกสารในทุกรูปแบบ ต้องมีการจัดเก็บและควบคุมตามระดับชั้นความลับ และระยะเวลาการจัดเก็บที่เหมาะสม

การส่งเสริมศักยภาพและทักษะความสามารถ (3.5.2)

- บริษัท เจ เอ็ม ที เน็ทเวอร์ค เซอร์วิสเซ็ส จำกัด (มหาชน) ต้องพิจารณาโอกาสในการส่งเสริมศักยภาพของบุคลากร ความพร้อมทางด้านทักษะในการดำเนินกิจกรรมให้บรรลุวัตถุประสงค์ และความคาดหวังในหน้าที่ความรับผิดชอบ