สำนักคอมพิวเตอร์ มหาวิทยาลัยศรีนครินทรวิโรฒ

คู่มือระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ
(Information Security Management System Manual)

รหัสเอกสาร :	ISMS-1PC-001
ชื่อเอกสาร :	คู่มือระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ (Information Security Management System Manual)
หมายเลขปรับปรุงเอกสาร :	2569-V.1.0
วันที่เอกสารมีผลบังคับใช้ :	2 กุมภาพันธ์ 2569
เจ้าของเอกสาร :	สำนักคอมพิวเตอร์ มหาวิทยาลัยศรีนครินทรวิโรฒ

หมายเลขข้อปฏิบัติสอดคล้องตามมาตรฐาน ISO/IEC 27001:2022

เอกสารฉบับนี้ ได้รับการจัดทำขึ้นเพื่อให้สอดคล้องกับมาตรฐาน ISO/IEC 27001:2022

ข้อกำหนด 4.4 Information security management system ระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ

ข้อกำหนด 5.2 Policy นโยบาย

ลายเซ็นรับรองเอกสาร

ผู้จัดทำ

ชื่อ - นามสกุล	ตำแหน่ง	ลายเซ็น	วันที่
นายมหัทธวัฒน์ รักษาเกียรติศักดิ์	หัวหน้างานระบบคอมพิวเตอร์และเครือข่าย		2 กุมภาพันธ์ 2569

ผู้ทบทวน

ชื่อ - นามสกุล	ตำแหน่ง	ลายเซ็น	วันที่
ผศ.ดร.กัลยกิตติ์ กีรติอังกูร	รักษาการแทนรองผู้อำนวยการ		2 กุมภาพันธ์ 2569

ผู้อนุมัติ

ชื่อ - นามสกุล	ตำแหน่ง	ลายเซ็น	วันที่
รศ.ดร.วุฒิพล ธาราธีรเศรษฐ์	รองอธิการบดีฝ่ายพัฒนากายภาพองครักษ์ รักษาการแทนผู้อำนวยการสำนักคอมพิวเตอร์		2 กุมภาพันธ์ 2569

ประวัติการแก้ไขเอกสาร

หมายเลขปรับปรุงเอกสาร (version):	รายละเอียด	ปรับปรุงโดย
2568-V.1.0	เริ่มจัดทำเอกสารใหม่ (จากมติที่ประชุมคณะกรรมการบริหารสำนักคอมพิวเตอร์ มหาวิทยาลัยศรีนครินทรวิโรฒ ครั้งที่ 1/2568)	7 มกราคม 2568
2568-V.2.0	เพิ่มเนื้อหา 12. แผนผังการสื่อสารภายในองค์กร“การแจ้งเหตุไปยัง สกมช. ....”	26 กุมภาพันธ์ 2568
2569-V.1.0	■ ปรับแก้ไขชื่อหัวหน้าฝ่ายระบบคอมพิวเตอร์และเครือข่ายเป็นหัวหน้างานระบบคอมพิวเตอร์และเครือข่าย ■ ปรับแก้ไขชื่อตำแหน่งจาก "รองผู้อำนวยการสำนักคอมพิวเตอร์" เป็น "รักษาการแทนรองผู้อำนวยการ" ■ ปรับแก้ไขชื่อตำแหน่งจาก "ผู้อำนวยการสำนักคอมพิวเตอร์" เป็น "รองอธิการบดีฝ่ายพัฒนากายภาพองครักษ์ รักษาการแทนผู้อำนวยการสำนักคอมพิวเตอร์" ■ ปรับแก้ไขรายละเอียด ข้อ 4.2 ข้อกำหนดเชิงกฎหมายและกฎระเบียบให้สอดคล้องกับแบบฟอร์มการวิเคราะห์ความสอดคล้องทางกฎหมายเพื่อลดความซ้ำซ้อน ของข้อมูล ■ ปรับแก้ไขรายละเอียดเอกสารอ้างอิง ข้อ 4.3 วัตถุประสงค์ระบบมาตรฐานสากล ISO/IEC 27001:2022 จากเอกสารรายการมาตรการด้านความมั่นคงปลอดภัยสารสนเทศที่นำมาประยุกต์ใช้ (Statement of Applicability) เป็น การวัดผลสัมฤทธิ์ของวัตถุประสงค์ (KPI measurement) ■ เพิ่มรูปภาพโครงสร้างคณะกรรมการและบุคลากรในระบบมาตรฐานการรักษาความมั่นคงปลอดภัย (Information Security Standards Organization Structure) ข้อ 9 และเพิ่มชื่อคณะทำงานด้านการบริหารจัดการเหตุการณ์ละเมิดความมั่นคงปลอดภัยสารสนเทศและปฏิบัติการระบบสารสนเทศ ■ ปรับแก้ไขรายละเอียดข้อ 10 การกำกับดูแล และหน้าที่ความรับผิดชอบให้สอดคล้องตามสำคั่งแต่งตั้ง ■ ตัดรายละเอียดแผนผังการสื่อสารภายในองค์กร ข้อ 13 ออก โดยนำรายละเอียดแผนผังดังกล่าวฯ ไปเพิ่มเติมในเอกสารISMS-3SD-003 Conmmunication Planเพื่อความสอดคล้องของข้อมูล	2 กุมภาพันธ์ 2569

สารบัญ

1. วัตถุประสงค์ (Objective)

สำนักคอมพิวเตอร์ตระหนักถึงความสำคัญของการรักษาความปลอดภัยด้านสารสนเทศ และมุ่งมั่นในการพัฒนาอย่างต่อเนื่องเพื่อยกระดับความมั่นคงปลอดภัยด้านสารสนเทศ จึงกำหนดนโยบายในแต่ละด้านไว้ดังต่อไปนี้

1.1 ยึดมั่นในการรักษาคุณลักษณะด้านความมั่นคงปลอดภัยของสารสนเทศ ได้แก่ การรักษาความลับ (Confidentiality) ความถูกต้องและครบถ้วน (Integrity) ความพร้อมในการใช้งาน (Availability) และการให้บริการอย่างต่อเนื่อง

1.2 การส่งเสริมความรู้ที่เพียงพอสำหรับการปฏิบัติงานและสร้างความตระหนักด้านความมั่นคงปลอดภัยทางสารสนเทศให้กับบุคลากรของสำนักคอมพิวเตอร์อย่างต่อเนื่อง

1.3 เพื่อใช้เป็นกรอบและแนวปฏิบัติในการป้องกันและรักษาสินทรัพย์ด้านสารสนเทศของสำนักคอมพิวเตอร์ มหาวิทยาลัยศรีนครินทรวิโรฒจากภาวะคุกคามทุกประเภทที่อาจจะเกิดขึ้นทั้งจากภายในและภายนอกมหาวิทยาลัยฯ โดยเจตนาหรือโดยรู้เท่าไม่ถึงการณ์ ซึ่งครอบคลุมด้านการรักษาความลับ ความถูกต้องครบถ้วน และสภาพพร้อมใช้งานของสารสนเทศ

2. ขอบเขต (Scope)

ห้องคอมพิวเตอร์กลาง สำนักคอมพิวเตอร์ มหาวิทยาลัยศรีนครินทรวิโรฒ (Data Center and Telecommunication Center) ชั้น 13 อาคาร นวัตกรรม ศาสตราจารย์ ดร.สาโรช บัวศรี

3. คำศัพท์และคำนิยาม (Terms and Definitions)

"มหาวิทยาลัย" หมายความว่า มหาวิทยาลัยศรีนครินทรวิโรฒ

"ส่วนงาน" หมายความว่า ส่วนงานตามพระราชบัญญัติมหาวิทยาลัยศรีนครินทรวิโรฒ

"หน่วยงานภายนอก" หมายความว่า องค์กรซึ่งมหาวิทยาลัยศรีนครินทรวิโรฒอนุญาตให้มีสิทธิในการเข้าถึงหรือใช้ข้อมูลหรือใช้ระบบงานที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศของมหาวิทยาลัย โดยจะได้รับสิทธิตามประเภทการใช้งานและต้องรับผิดชอบในการไม่เปิดเผยความลับของมหาวิทยาลัยโดยมิได้รับอนุญาต

"สารสนเทศ" หมายความว่า ข้อมูลที่ผ่านการประมวลผลแล้ว การจัดระเบียบให้ข้อมูล ซึ่งอยู่ในรูปของตัวเลข ข้อความ หรือภาพกราฟิก ให้อยู่ในลักษณะที่ผู้ใช้สามารถเข้าใจได้ง่าย และสามารถ นำไปใช้ประโยชน์ในการบริหาร การวางแผนการตัดสินใจ และอื่น ๆ ได้

"ข้อมูล" หมายความว่า ข้อมูล ข้อความ คำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใดบรรดาที่อยู่ในระบบคอมพิวเตอร์ในสภาพที่ระบบคอมพิวเตอร์อาจประมวลผลได้ และให้หมายความรวมถึงข้อมูล อิเล็กทรอนิกส์ ตามกฎหมายว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ด้วย

"เทคโนโลยีสารสนเทศและการสื่อสาร" (Information and communication technology) หมายความว่า เทคโนโลยีสำหรับการประมวลผลสารสนเทศ ซึ่งจะครอบคลุมถึงการรับส่ง แปลง ประมวลผล และสืบค้นสารสนเทศ โดยมีองค์ประกอบ 3 ส่วนคือ คอมพิวเตอร์ การสื่อสาร และสารสนเทศ ซึ่งต้องอาศัยการทำงานร่วมกัน

“ระบบคอมพิวเตอร์" หมายความว่า อุปกรณ์หรือชุดอุปกรณ์ของคอมพิวเตอร์ที่เชื่อมการทำงานเข้าด้วยกัน โดยได้มีการกำหนดคำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใด และแนวทางปฏิบัติงานให้อุปกรณ์หรือชุดอุปกรณ์ทำหน้าที่ประมวลผลข้อมูลโดยอัตโนมัติ

"ระบบสารสนเทศ" หมายถึง ชุดขององค์ประกอบที่ทำหน้าที่รวบรวม ประมวลผล จัดเก็บ และแจกจ่ายสารสนเทศ เพื่อช่วยการตัดสินใจและการควบคุมในองค์กร ในการทำงานของระบบสารสนเทศ ประกอบไปด้วยกิจกรรม 3 อย่าง คือ การนำข้อมูลเข้าสู่ระบบ (Input) การประมวลผล (Processing) และการนำเสนอผลลัพธ์ (Output)

"ระบบงาน" หมายความว่า การนำระบบสารสนเทศมาประยุกต์ใช้ในการทำงานเพื่อให้งานสำเร็จตามวัตถุประสงค์ที่ตั้งไว้ อาทิ ระบบงานบุคคล ระบบจัดเก็บเอกสาร

"ระบบปฏิบัติการ" (operating system) หมายความว่า ซอฟต์แวร์ควบคุมการทำงานของเครื่องคอมพิวเตอร์ และจัดสรรการใช้ทรัพยากรระบบ ซึ่งได้แก่ การจัดการหน่วยความจำ การควบคุมการทำงานของอุปกรณ์ป้อนข้อมูล (แป้นพิมพ์ เมาส์) และอุปกรณ์แสดงผล (จอภาพ เครื่องพิมพ์)

"ระบบเครือข่าย" (network) หมายความว่า ระบบเครือข่ายคอมพิวเตอร์ของมหาวิทยาลัยศรีนครินทรวิโรฒ

"เครื่องคอมพิวเตอร์แม่ข่าย" (server) หมายความว่า เครื่องคอมพิวเตอร์ในระบบเครือข่ายที่ทำหน้าที่เป็นศูนย์กลางของการทำงาน อาทิ จัดเก็บข้อมูลหรือซอฟต์แวร์ สำหรับให้บริการ แก่เครื่องคอมพิวเตอร์อื่น ๆ หรือควบคุมการทำงานในเครือข่าย

"สินทรัพย์" (asset) หมายความว่า เครื่องคอมพิวเตอร์ของมหาวิทยาลัย เครือข่ายย่อย ข้อมูลและระบบสารสนเทศต่าง ๆ ที่มหาวิทยาลัยพัฒนาหรือจัดหาเพื่อใช้ในการดำเนินการของมหาวิทยาลัย

"ความมั่นคงปลอดภัยของสารสนเทศ" (Information Security) หมายความว่า การธำรงไว้ซึ่งความลับ (Confidentiality) ความถูกต้องครบถ้วน (Integrity) และสภาพพร้อมใช้งาน (Availability) ของสารสนเทศ รวมทั้งคุณสมบัติอื่น ได้แก่ ความถูกต้องแท้จริง (Authenticity) ความรับผิด (Accountability) การห้ามปฏิเสธความรับผิด (Non-repudiation) และความน่าเชื่อถือ (Reliability)

"ความลับ" (Confidentiality) หมายความว่า การรับรองว่าจะมีการเก็บรักษาข้อมูลไว้ เป็นความลับ และจะมีเพียงผู้มีสิทธิเท่านั้นที่จะสามารถเข้าถึงข้อมูลเหล่านั้นได้

"ความถูกต้องครบถ้วน" (Integrity) หมายความว่า การรับรองว่าข้อมูลจะไม่ถูกกระทำการใด ๆ อันมีผลให้เกิดการเปลี่ยนแปลง หรือแก้ไขโดยผู้ไม่มีสิทธิ ไม่ว่าการกระทำนั้นจะมีเจตนาหรือไม่ก็ตาม

"สภาพพร้อมใช้งาน" (Availability) หมายความว่า การรับรองได้ว่าข้อมูล หรือระบบสารสนเทศ ทั้งหลายพร้อมที่จะให้บริการในเวลาที่ต้องการใช้งาน

"เหตุการณ์ด้านความมั่นคงปลอดภัย" (Information Security Event) หมายความว่า กรณีที่ระบุการเกิดเหตุการณ์ สภาพของบริการหรือเครือข่ายที่แสดงให้เห็นความเป็นไปได้ ที่จะเกิดการฝ่าฝืนนโยบายด้านความมั่นคงปลอดภัยหรือมาตรการป้องกันที่ล้มเหลว หรือเหตุการณ์อันไม่อาจรู้ได้ว่าอาจเกี่ยวข้องกับความมั่นคงปลอดภัย

"สถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด" (Information Security Incident) หมายความว่า สถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์ หรือไม่อาจคาดคิด

ซึ่งอาจทำให้ระบบของมหาวิทยาลัยถูกบุกรุก หรือโจมตี และความมั่นคงปลอดภัยถูกคุกคาม

"ความเสี่ยง" หมายความว่า โอกาสของสินทรัพย์สารสนเทศในการถูกละเมิดการ รักษาความ ปลอดภัย

"ช่องโหว่" (Vulnerability) หมายความว่า จุดอ่อนของระบบสารสนเทศทำให้ผู้ไม่ประสงค์ดีเข้าโจมตีระบบทำให้ประสิทธิภาพของการทำงานลดลง

"การเข้าถึงหรือควบคุมการใช้งานสารสนเทศ" (Access Control) หมายความว่า การอนุญาตการกำหนดสิทธิ หรือการมอบอำนาจให้ผู้ใช้งานเข้าถึง หรือใช้งานเครือข่าย หรือระบบสารสนเทศทั้งทางอิเล็กทรอนิกส์และทางกายภาพ รวมทั้งการอนุญาตเช่นว่านั้นสำหรับบุคคลภายนอก ตลอดจนอาจกำหนดข้อปฏิบัติเกี่ยวกับการเข้าถึงโดยมิชอบเอาไว้ด้วยก็ได้

"การเข้าถึงจากระยะไกล" (Remote Access) หมายความว่า การที่เครื่องคอมพิวเตอร์หรือ ระบบเครือข่ายเชื่อมต่อ เข้ากับเครื่องคอมพิวเตอร์หรือเครือข่ายอื่นผ่านอุปกรณ์สื่อสาร หรือสื่อสัญญาณอื่น ๆ อาทิ โมเด็ม (Modem) วีพีเอ็น (VPN หรือ Virtual Private Network)

"ผู้ใช้งาน" หมายความว่า นิสิตและบุคลากรของมหาวิทยาลัยศรีนครินทรวิโรฒที่ได้รับสิทธิ ในการใช้งานระบบสารสนเทศของมหาวิทยาลัย รวมถึงบุคคลจากหน่วยงานภายนอก ซึ่งได้รับอนุญาต ให้เข้าใช้งานสารสนเทศของมหาวิทยาลัย

"บัวศรีไอดี" (Buasi ID) หมายความว่า ชื่อและรหัสบัญชีใช้งานเพื่อใช้ในการพิสูจน์ตัวตนก่อนการเข้าใช้เครือข่ายและบริการระบบสารสนเทศของมหาวิทยาลัย

"รหัสผ่าน" (Password) หมายความว่า ตัวอักษรหรืออักขระหรือตัวเลข ที่ใช้เป็นเครื่องมือในการตรวจสอบยืนยันตัวบุคคล เพื่อควบคุมการเข้าถึงข้อมูลและระบบข้อมูลในการรักษา ความมั่นคง ปลอดภัยของข้อมูลและระบบสารสนเทศ

"สิทธิของผู้ใช้งาน" หมายความว่า สิทธิทั่วไป สิทธิจำเพาะ สิทธิพิเศษ และสิทธิอื่นใดที่เกี่ยวข้องกับระบบสารสนเทศของส่วนงาน

"Idle Timeout" หมายความว่า ระยะเวลาที่ผู้ใช้งานเชื่อมต่อกับระบบสารสนเทศ และไม่มีการใช้งานเกินระยะเวลาที่กำหนด ระบบสารสนเทศจะทำการตัดการเชื่อมต่อผู้ใช้งานออกจากระบบ

"Session Timeout" หมายความว่า ระยะเวลาที่ผู้ใช้สามารถเชื่อมต่อกับระบบสารสนเทศได้

4. นโยบายสำหรับระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ

ในการดำเนินงานบนระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ จะต้องเป็นไปตาม ข้อกำหนดด้านความมั่นคงปลอดภัยในแต่ละด้าน ดังต่อไปนี้

4.1 ข้อกำหนดตามการกำหนดค่าเป้าหมายและการรายงานผลการปฏิบัติงานตามตัวชี้วัด (KPI)

ระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ จำเป็นต้องวัดผลประสิทธิภาพได้ โดยใช้ตัวชี้วัดที่มีความสอดคล้องกับนโยบายหน่วยงาน ความเสี่ยง ตลอดจนการวัดประสิทธิภาพของมาตรการควบคุมเชิงความปลอดภัยสารสนเทศที่สำนักคอมพิวเตอร์ มหาวิทยาลัยศรีนครินทรวิโรฒได้นำมาใช้ ทั้งนี้ผลประสิทธิภาพต้องได้รับการรายงานแก่ คณะผู้บริหารและสื่อสารไปถึงทุกหน่วยงานที่เกี่ยวข้องโดยกำหนดให้การวัดผลประสิทธิภาพ ของระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศต้องจัดทำขึ้นอย่างน้อย 1 ครั้งต่อปี โดยตัวชี้วัดต้องครอบคลุมทุกหน่วยงานภายใต้ขอบเขตการดำเนินงาน

อ้างอิง : เอกสารการวัดผลสัมฤทธิ์ของวัตถุประสงค์ (KPI measurement) (ISMS-3SD-002)

4.2 ข้อกำหนดเชิงกฎหมายและกฎระเบียบที่เกี่ยวข้อง

ระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ ต้องมีความสอดคล้องตามข้อกำหนด กฎหมาย กฎระเบียบบังคับ ตลอดจนนโยบายทั้งภายในและภายนอก สำนักคอมพิวเตอร์ มหาวิทยาลัยศรีนครินทรวิโรฒ ที่มีส่วนเกี่ยวข้องทั้งโดยตรงและโดยอ้อมในการดำเนินกิจกรรม โดยเป็นหน้าที่สำคัญของบุคลากรทุกคนภายใต้ขอบเขตการดำเนินงานที่ต้องศึกษาทำความเข้าใจกับข้อกำหนดต่าง ๆ โดยรายละเอียด

รายการข้อกฎหมายที่เกี่ยวข้องกับระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ ได้ทำการวิเคราะห์ความสอดคล้องไว้ เพื่อให้มั่นใจว่าสำนักคอมพิวเตอร์ปฏิบัติตามข้อกำหนด กฎหมาย กฎระเบียบบังคับที่เกี่ยวข้องอย่างมีประสิทธิภาพ

อ้างอิง : แบบฟอร์มการวิเคราะห์ความสอดคล้องทางกฎหมาย (Legal Compliance Analysis Form) (ISMS-3FM-030)

4.3 วัตถุประสงค์ระบบมาตรฐานสากล ISO/IEC 27001:2022

เพื่อเป็นการทบทวนว่าได้มีการปฏิบัติตามระบบบริหารงานที่ได้วางแผนไว้ได้อย่างมีประสิทธิภาพและบรรลุตามวัตถุประสงค์ที่ตั้งไว้ จึงได้มีการมอบหมายให้มีการจัดตั้งคณะทำงาน เพื่อดำเนินการ กำหนด

เป้าหมายให้สอดคล้องกับ นโยบาย วิสัยทัศน์ พันธกิจ สมรรถนะหลัก ค่านิยม บริบท ความต้องการ ความคาดหวัง ความเสี่ยง และกระบวนการทำงาน รวมถึงรายการมาตรการควบคุมที่นำมาประยุกต์ใช้

อ้างอิง : เอกสารการวัดผลสัมฤทธิ์ของวัตถุประสงค์ (KPI measurement) (ISMS-3SD-002)

4.4 ข้อกำหนดตามนโยบาย คำสั่งราชการ เอกสารอื่น ๆ

ระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศต้องมีความสอดคล้องกับข้อกำหนดอื่น ๆ ที่มีผลต่อระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศทั้งทางตรงและทางอ้อม โดยให้ผู้รับผิดชอบในการดูแลนั้นพิจารณาสร้างความสอดคล้องตามแนวทางอันเหมาะสม โดยมุ่งเน้นความสอดคล้อง ต่อรายการประกาศ ดังต่อไปนี้

4.4.1 ประกาศมหาวิทยาลัยศรีนครินทรวิโรฒ เรื่องนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ พ.ศ. 2565

5. หลักการความมั่นคงปลอดภัยสารสนเทศ

ระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ ใช้แนวทางความมั่นคงปลอดภัยสารสนเทศ โดยพิจารณา 3 องค์ประกอบหลัก ได้แก่

องค์ประกอบ	คำอธิบาย
ความลับ (Confidentiality)	การปกป้องข้อมูลหรือระบบให้สามารถเข้าถึงได้เฉพาะผู้ที่มีสิทธิ์เท่านั้น
ความสมบูรณ์ (Integrity)	การป้องกันไม่ให้ข้อมูลหรือระบบถูกดัดแปลงแก้ไขโดยไม่ได้รับอนุญาต และการตรวจสอบให้แน่ใจว่าข้อมูลที่เก็บหรือส่งต่อยังคงความถูกต้อง และครบถ้วน
ความพร้อมใช้ (Availability)	การทำให้ข้อมูลหรือระบบสามารถเข้าถึงและใช้งานได้เมื่อผู้ใช้ต้องการ

โดยองค์ประกอบข้างต้นจะถูกนำมาพิจารณาเป็นมูลค่าของสินทรัพย์สารสนเทศในเชิงความมั่นคงปลอดภัยอันรวมไปถึงสินทรัพย์อื่น ๆ ที่เกี่ยวข้องกับสารสนเทศทั้งนี้ข้อมูลสารสนเทศ รวมถึงข้อมูลในรูปแบบไฟล์อิเล็กทรอนิกส์ เอกสารกระดาษ หรือข้อมูลที่เกิดจากการสนทนาระหว่างบุคคล ซึ่งจะต้องจัดทำแนวทางในการจัดการข้อมูลสารสนเทศในแต่ละรูปแบบให้เหมาะสมต่อไป

6. ความมั่นคงปลอดภัยสารสนเทศบนพื้นฐานของความเสี่ยง (Information Security Aspects to Risk Based Approach)

สำนักคอมพิวเตอร์ มหาวิทยาลัยศรีนครินทรวิโรฒจะต้องจัดให้มีประเมินความเสี่ยง ของทรัพย์สินสารสนเทศภายในขอบเขตการดำเนินงานระบบ ISMS ให้สอดคล้องกับนโยบายการ บริหารความเสี่ยงมหาวิทยาลัยศรี

นครินทรวิโรฒ เพื่อให้ทราบถึงสภาวะความเสี่ยงที่มีในปัจจุบัน ทั้งนี้ ความเสี่ยงใด ๆ ที่มากกว่าระดับความเสี่ยงที่ยอมรับได้ (Risk Appetite Statement : RAS) จะต้องได้รับการจัดทำแผนงาน เพื่อจัดการความเสี่ยงดังกล่าวให้อยู่ในระดับที่เหมาะสมต่อไป

นอกเหนือจากการประเมินความเสี่ยงของทรัพย์สินสารสนเทศแล้วจะต้องมีการประเมินผลกระทบ ต่อการใช้งานระบบงานสารสนเทศของระบบงานหรือบริการต่าง ๆ ที่อยู่ภายในขอบเขตการดำเนินงานเพื่อให้ทราบระดับความสำคัญของระบบงานโดยเกณฑ์ที่ใช้ในการประเมินผลกระทบ ดังกล่าว มีดังต่อไปนี้

- ความเสี่ยง ด้านการดำเนินงาน (Operational Risk)
- ความเสี่ยง ด้านชื่อเสียง (Reputation Risk)

สำหรับการกำหนดระดับความเสี่ยงที่ยอมรับได้ (Risk Appetite Statement : RAS) กำหนดให้ผู้แทนกรรมการบริหารจัดการความมั่นคงปลอดภัยข้อมูลสารสนเทศ (ISMS Management Representative: ISMR) เป็นผู้พิจารณาระดับความเสี่ยงที่เหมาะสม โดยใช้เกณฑ์ดังต่อไปนี้

- ระดับความเสี่ยงที่ยอมรับได้ จะต้องไม่ขัดต่อข้อกำหนดเชิงกฎหมายที่เกี่ยวข้องกับการ ให้บริการภายใน สำนักคอมพิวเตอร์ มหาวิทยาลัยศรีนครินทรวิโรฒ
- ระดับความเสี่ยงที่ยอมรับได้จะต้องไม่ขัดกับนโยบายขององค์กร
- ระดับความเสี่ยงที่ยอมรับได้ (Risk Appetite Statement: RAS) จะต้องมีการทบทวนเป็นประจำทุกปี และใช้เป็นแนวทางในการกำหนดกลยุทธ์ในการบริหารจัดการความเสี่ยง

อ้างอิง : เอกสารระเบียบขั้นตอนการบริหารจัดการความเสี่ยง (Risk Management Methodology) (ISMS-1PC-003)

สำนักคอมพิวเตอร์ มหาวิทยาลัยศรีนครินทรวิโรฒ ต้องพิจารณาถึงความเสี่ยงด้านข้อมูลสารสนเทศ เป็นสำคัญเพื่อพิจารณาถึงการเลือกใช้มาตรการควบคุมหรือการกำหนดนโยบายต่าง ๆ ให้เกิดความสอดคล้อง โดยให้มุ่งเน้นถึงผลกระทบในทุกด้านที่เกี่ยวข้อง และระดับการควบคุมป้องกันภัยคุกคามที่เหมาะสม

7. เป้าหมายของความมั่นคงปลอดภัยสารสนเทศ

ระบบสารสนเทศของ สำนักคอมพิวเตอร์ มหาวิทยาลัยศรีนครินทรวิโรฒ มีความมั่นคง ปลอดภัย เชื่อถือได้ และพร้อมใช้งานตลอดเวลา

8. การจัดทำกลยุทธ์ด้านความมั่นคงปลอดภัยสารสนเทศ

กลยุทธ์ด้านความมั่นคงปลอดภัยมีการกำหนดขึ้น เพื่อสร้างกรอบการปฏิบัติแก่ผู้ปฏิบัติงาน ภายใต้ขอบเขต โดยการเข้าใจถึงวัตถุประสงค์และแนวทางที่สามารถใช้ในการดำเนิน กิจกรรม โดยมีการกำหนดกลยุทธ์ ดังต่อไปนี้

8.1 ความสามารถในการปรับเปลี่ยนเพื่อสร้างความสอดคล้อง (Flexibility)

ระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ ควรถูกออกแบบให้มีความเหมาะสม กับสภาวะแวดล้อมของสำนักคอมพิวเตอร์ มหาวิทยาลัยศรีนครินทรวิโรฒ สามารถเปลี่ยนแปลง ตามปัจจัยต่าง ๆ เพื่อรองรับการทำงานของบุคลากรได้อย่างมีประสิทธิภาพ

8.2 ความสม่ำเสมอในการบังคับใช้มาตรฐานความมั่นคงปลอดภัยสารสนเทศ (Uniformity)

เพื่อให้ระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศทำงานได้อย่างมีประสิทธิภาพ ควรมีการบังคับใช้มาตรฐานความมั่นคงปลอดภัยภายใน สำนักคอมพิวเตอร์ มหาวิทยาลัยศรีนครินทรวิโรฒ อย่างสม่ำเสมอ

8.3 ระบบบริหารจัดการความมั่นคงปลอดภัยบนพื้นฐานของความเสี่ยง (Risk Based Approach)

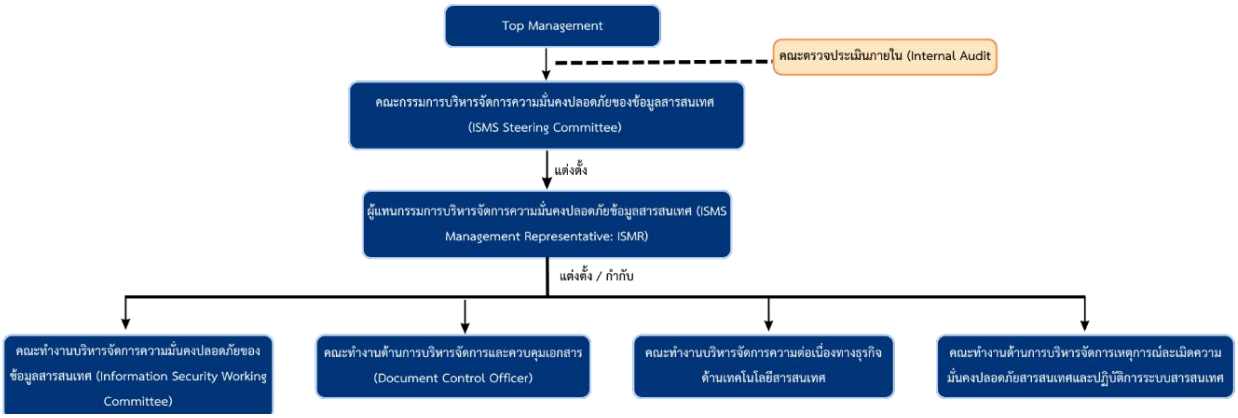
สำนักคอมพิวเตอร์ มหาวิทยาลัยศรีนครินทรวิโรฒ ต้องพิจารณาถึงความเสี่ยงด้านข้อมูล สารสนเทศเป็นสำคัญ เพื่อพิจารณาถึงการเลือกใช้มาตรการควบคุมหรือการกำหนดนโยบายต่าง ๆ ให้เกิดความสอดคล้องโดยให้มุ่งเน้นถึงผลกระทบในทุกด้านที่เกี่ยวข้อง และระดับการ ควบคุม ป้องกันภัยคุกคามที่เหมาะสม

8.4 การส่งเสริมศักยภาพบุคลากร และทักษะที่จำเป็นในการรับมือความมั่นคงปลอดภัยสารสนเทศ

สำนักคอมพิวเตอร์ มหาวิทยาลัยศรีนครินทรวิโรฒต้องมั่นใจว่าบุคลากรภายใต้ ขอบเขตระบบ บริหารจัดการความมั่นคงปลอดภัยสารสนเทศ มีทักษะความสามารถเพียงพอ ต่อการทำกิจกรรมต่าง ๆ โดยทักษะความสามารถแบ่งออกเป็น

- ทักษะเฉพาะทางและความชำนาญพิเศษตามสายงาน
    - การดูแลรักษาเครื่องคอมพิวเตอร์แม่ข่าย ระบบสนับสนุนโครงสร้างพื้นฐาน และระบบเครือข่าย เพื่อความมั่นคงปลอดภัย
    - การบริหารจัดการ Supplier
    - การรองรับเหตุการณ์ละเมิดความมั่นคงปลอดภัย การเก็บรวบรวมหลักฐานทางด้านไอที
    - การบริหารจัดการความต่อเนื่องทางธุรกิจ (Business Continuity Management)
- ทักษะด้านความมั่นคงปลอดภัยสารสนเทศและระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ
    - ความเข้าใจในระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ
    - ความเข้าใจในกระบวนการบริหารจัดการความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศ

9. โครงสร้างคณะกรรมการและบุคลากรในระบบมาตรฐานการรักษาความมั่นคงปลอดภัย (Information Security Standards Organization Structure)



ภาพที่ 1 โครงสร้างคณะกรรมการและบุคคลการในระบบมาตรฐานการรักษาความมั่นคงปลอดภัย

การดำเนินการระบบมาตรฐานสากล จะต้องมีการกำหนดโครงสร้างคณะทำงาน ดังนี้

1. คณะกรรมการบริหารจัดการความมั่นคงปลอดภัยของข้อมูลสารสนเทศ (ISMS Steering Committee)
2. ผู้แทนคณะกรรมการบริหารจัดการด้านความมั่นคงปลอดภัยของข้อมูล (Information Security Management Representative)
3. คณะทำงานบริหารจัดการความมั่นคงปลอดภัยของข้อมูลสารสนเทศ (Information Security Working Committee)
4. คณะตรวจประเมินภายใน (Internal Audit)
5. ผู้ควบคุมเอกสาร (Document Control Officer : DCO)
6. คณะทำงานบริหารจัดการความต่อเนื่องทางธุรกิจด้านเทคโนโลยีสารสนเทศ
7. คณะทำงานด้านการบริหารจัดการเหตุการณ์ละเมิดความมั่นคงปลอดภัยสารสนเทศและปฏิบัติการระบบสารสนเทศ

10. การกำกับดูแล และหน้าที่ความรับผิดชอบ

10.1 คณะกรรมการบริหารจัดการความมั่นคงปลอดภัยข้อมูลสารสนเทศ (ISMS Steering Committee)

คณะกรรมการบริหารจัดการความมั่นคงปลอดภัยข้อมูลสารสนเทศ (ISMS Steering Committee) มีหน้าที่ในการวางแผน จัดการสนับสนุนให้ทุกกิจกรรมที่ เกี่ยวข้อง กับความมั่นคงปลอดภัยสารสนเทศเป็นไปตามข้อกำหนดในนโยบาย ทั้งนี้ คณะกรรมการบริหารจัดการความมั่นคงปลอดภัยข้อมูลสารสนเทศ (ISMS Steering Committee) ต้องดำเนินการ ดังต่อไปนี้

1. แต่งตั้งผู้แทนคณะกรรมการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ (Information Security Management Representative : ISMR) เพื่อดำเนินการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศของห้องคอมพิวเตอร์กลาง (Data Center)
2. พิจารณานโยบายและกำหนดทิศทางในการดำเนินการให้มีประสิทธิภาพตามระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ
3. พิจารณาอนุมัติเป้าหมายและวัตถุประสงค์ของการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ
4. พิจารณาอนุมัติขั้นตอนปฏิบัติ (Procedure) ภายใต้ระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศของห้องคอมพิวเตอร์กลาง(Data Center)
5. พิจารณาแนวทางและวิธีการประเมินความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศ
6. พิจารณาอนุมัติแผนการสื่อสารภายใต้ระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ
7. กำหนดหลักเกณฑ์ระดับความเสี่ยงที่ยอมรับได้ในกระบวนการบริหารความเสี่ยงสำหรับการดำเนินการบริหารจัดการด้านความมั่นคงปลอดภัยสารสนเทศ
8. สนับสนุนทรัพยากรที่จำเป็นเพื่อให้บรรลุวัตถุประสงค์ในการรักษาความมั่นคงปลอดภัยสารสนเทศของสำนักคอมพิวเตอร์ มหาวิทยาลัยศรีนครินทรวิโรฒ
9. แต่งตั้งคณะตรวจสอบภายใน และคณะทำงานอื่นใดตามความจำเป็นและเหมาะสม
10. พิจารณา และรับรองการดำเนินการตามมาตรฐานการควบคุมด้านความมั่นคงปลอดภัยสารสนเทศ (Information Security Controls)
11. รายงานผลการดำเนินงานต่อประจำสำนักคอมพิวเตอร์ อย่างน้อยปีละ 1 ครั้ง

10.2 ผู้แทนกรรมการบริหารจัดการความมั่นคงปลอดภัยข้อมูลสารสนเทศ (ISMS Management Representative: ISMR)

ผู้แทนกรรมการบริหารจัดการความมั่นคงปลอดภัยข้อมูลสารสนเทศ (ISMR) มีหน้าที่รายงานผลการดำเนินการต่อคณะกรรมการบริหารจัดการความมั่นคงปลอดภัยข้อมูลสารสนเทศ (ISMS Steering Committee) โดยมีความรับผิดชอบดังต่อไปนี้

1. เป็นผู้แทนของคณะกรรมการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ (ISMS Steering Committee) ในการดำเนินการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศของห้องคอมพิวเตอร์กลาง (Data Center)
2. จัดทำและทบทวนแนวนโยบายภายใต้ระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศของห้องคอมพิวเตอร์กลาง (Data Center) เพื่อพัฒนาระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ
3. จัดทำและทบทวนเป้าหมายและวัตถุประสงค์ของการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ

4. จัดทำและทบทวนขั้นตอนปฏิบัติ (Procedure) ภายใต้ระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศของห้องคอมพิวเตอร์กลาง (Data Center)
5. จัดทำและทบทวนวิธีการบริหารจัดการความเสี่ยง (Risk Management Methodology) และระดับความเสี่ยงที่สำนักคอมพิวเตอร์ยอมรับได้
6. จัดทำและทบทวนแผนการสื่อสารภายใต้ระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ ของห้องคอมพิวเตอร์กลาง (Data Center)
7. บริหารจัดการทรัพยากรบุคคลและทรัพยากรอื่นที่เกี่ยวข้อง ทบทวนขีดความสามารถที่จำเป็น ของบุคลากร และกำหนดแผนการฝึกอบรมด้านสารสนเทศและการรักษาความปลอดภัยสารสนเทศ ภายในขอบเขตของระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ
8. ติดตามการดำเนินงานและประสานงานกับคณะทำงานที่เกี่ยวข้องในการเฝ้าระวัง ทบทวน รักษา และปรับปรุงระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศให้มีความมั่นคงปลอดภัยอยู่เสมอ
9. จัดทำ ติดตาม และตรวจสอบผลการดำเนินการตามตัวชี้วัดประสิทธิภาพของระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศในส่วนที่เกี่ยวข้องกับผู้แทนคณะกรรมการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ
10. เชิญบุคคลที่เกี่ยวข้องมาให้ข้อมูล ข้อเท็จจริง และข้อเสนอแนะ รวมทั้งจัดส่งเอกสารหลักฐานที่เกี่ยวข้องเพื่อประกอบการพิจารณาของผู้แทนคณะกรรมการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ
11. แต่งตั้งคณะทำงานตามความจำเป็นและเหมาะสม
12. รายงานผลการดำเนินงานการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศต่อผู้แทนคณะกรรมการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศอย่างน้อยปีละ 1 ครั้ง
13. ปฏิบัติงานอื่นใดตามที่คณะกรรมการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศมอบหมาย

10.3 คณะทำงานปฏิบัติการงานบริหารจัดการความมั่นคงปลอดภัยข้อมูลสารสนเทศ (ISMS Working Committee)

คณะทำงาน ISMS คือผู้ประสานงานผู้แทนกรรมการบริหารจัดการความมั่นคง ปลอดภัย ข้อมูลสารสนเทศ (ISMR) โดยให้คำแนะนำการดำเนินงานที่ เกี่ยวข้อง กับความ มั่นคง ปลอดภัยสารสนเทศในสำนักคอมพิวเตอร์ มหาวิทยาลัย ศรีนครินทรวิโรฒ ประกอบไปด้วย

1. ดำเนินการตามนโยบาย พร้อมรายงานผลการปฏิบัติงาน และติดตามความคืบหน้าของการดำเนินงานตามที่คณะกรรมการบริหารระบบมาตรฐานสากลได้กำหนดไว้ เพื่อให้เป็นไปอย่างมีประสิทธิภาพ

2. จัดการฝึกอบรมเพื่อเสริมสร้างความรู้และความเข้าใจให้กับเจ้าหน้าที่ที่เกี่ยวข้อง เพื่อสร้างความตระหนักถึงความสำคัญของระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ (ISO/IEC 27001:2022)
3. จัดทำและทบทวนคู่มือคุณภาพตามระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ (ISO/IEC 27001:2022) เพื่อนำเสนอต่อคณะกรรมการบริหารจัดการความมั่นคงปลอดภัยข้อมูลสารสนเทศ
4. ประเมินความเสี่ยงตามวิธีที่กำหนด จัดทำรายงานการประเมินความเสี่ยง พร้อมทั้งแผนการจัดการความเสี่ยง ดำเนินการตามแผนที่วางไว้ รวมถึงสรุปมาตรการควบคุมและแผนความต่อเนื่องทางธุรกิจ พร้อมประเมินประสิทธิภาพ เพื่อเสนอแนวทางปรับปรุงต่อคณะกรรมการบริหารบริหารจัดการความมั่นคงปลอดภัยข้อมูลสารสนเทศ
5. จัดเตรียมข้อมูลให้กับทีมตรวจสอบภายในระบบ ระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ (ISO/IEC 27001:2022) (Internal Audit)
6. จัดทำและทบทวนเอกสารขั้นตอนการปฏิบัติงานหรือเอกสารสนับสนุนอื่น ๆ เพื่อให้สอดคล้องกับการปฏิบัติงานจริงและทันสมัยอยู่เสมอ
7. ตรวจสอบให้ระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ (ISO/IEC27001:2022) ดำเนินการอย่างต่อเนื่องและถูกต้องตามกระบวนการ เพื่อรองรับการตรวจสอบจากผู้ให้การรับรอง
8. ควบคุมการจัดเก็บ ดูแล เผยแพร่ และปรับปรุงเอกสารที่เกี่ยวข้องกับระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ (ISO/IEC 27001:2022)

10.4 คณะทำงานด้านการบริหารจัดการและควบคุมเอกสาร (Document Control Officer)

โดยมีความรับผิดชอบ ดังต่อไปนี้

1. จัดการเก็บรักษา ดูแล และเผยแพร่เอกสารภายในองค์กร และ/หรือ เอกสารที่มาจากภายนอกซึ่งเกี่ยวข้องกับระบบการบริหารจัดการ
2. ควบคุมการปรับปรุงแก้ไขและเปลี่ยนแปลงเอกสารที่เกี่ยวข้องกับระบบการจัดการด้านความมั่นคงปลอดภัยสารสนเทศ
3. ปฏิบัติงานอื่นใดตามที่คณะกรรมการบริหารจัดการความมั่นคงปลอดภัยข้อมูลสารสนเทศมอบหมาย

10.5 คณะตรวจประเมินภายใน (Internal Audit)

โดยมีความรับผิดชอบ ดังต่อไปนี้

1. จัดทำแผนการตรวจประเมินระบบบริหารจัดการความมั่นคงปลอดภัยข้อมูลสารสนเทศอย่างน้อยปีละ 1 ครั้ง
2. จัดให้มีกิจกรรมการตรวจประเมินตามแผนที่กำหนดใน (ข้อ 1)

3. ดำเนินการตรวจประเมินตามแผนการที่กำหนดใน (ข้อ 1)
4. ติดตามและตรวจสอบผลการแก้ไขและการป้องกันประเด็นความไม่สอดคล้องที่พบจากการตรวจประเมินภายใน (Internal Audit) หรือการตรวจประเมินภายนอก (External Audit)
5. จัดอบรมผู้ตรวจประเมินให้มีความรู้ความสามารถในการตรวจประเมินระบบบริหารจัดการความมั่นคงปลอดภัยข้อมูลสารสนเทศอย่างน้อยปีละ 1 ครั้ง
6. เชิญบุคคลที่เกี่ยวข้องมาให้ข้อมูล ข้อเท็จจริง และข้อเสนอแนะ รวมทั้งจัดส่งเอกสารหลักฐานที่เกี่ยวข้อง เพื่อประกอบการพิจารณาของคณะตรวจสอบภายใน
7. รายงานผลการดำเนินงานและผลการตรวจประเมินต่อคณะกรรมการบริหารจัดการความมั่นคงปลอดภัยข้อมูลสารสนเทศผ่านผู้แทนคณะกรรมการบริหารจัดการความมั่นคงปลอดภัยข้อมูลสารสนเทศอย่างน้อยปีละ 1 ครั้ง
8. ดำเนินการร่วมกับผู้แทนกรรมการบริหารจัดการความมั่นคงปลอดภัยข้อมูลสารสนเทศ ในการติดต่อกับหน่วยงานที่ให้การรับรอง เพื่อวางแผนและกำหนดแผนในการตรวจประเมินบริหารจัดการความมั่นคงปลอดภัยภัยมูลสารสนเทศ ตามมาตรฐาน ISO/IEC 27001:2022

10.6 คณะทำงานบริหารจัดการความต่อเนื่องทางธุรกิจด้านเทคโนโลยีสารสนเทศ

โดยมีความรับผิดชอบ ดังต่อไปนี้

1. ดำเนินการจัดทำ ทบทวน และปรับปรุงบทวิเคราะห์ผลกระทบทางธุรกิจ การประเมินความเสี่ยง และแผนบริหารความต่อเนื่องทางธุรกิจด้านเทคโนโลยีสารสนเทศ รวมถึงกระบวนการและเอกสารที่เกี่ยวข้อง ให้มีความทันสมัยและสอดคล้องกับเทคโนโลยีสารสนเทศและภัยคุกคามปัจจุบัน
2. กำหนดระบบงานและกระบวนการที่มีความสำคัญต่อการบริหารจัดการความต่อเนื่องทางธุรกิจด้านเทคโนโลยีสารสนเทศภายใต้ขอบเขตและแนวนโยบายที่คณะกรรมการบริหารจัดการความต่อเนื่องทางธุรกิจด้านเทคโนโลยีสารสนเทศกำหนด
3. จัดทำแผนการกู้คืนระบบ กำหนดระยะเวลาในการกู้คืนระบบและระบบงานที่เกี่ยวข้อง และวางกลยุทธ์ในการกู้คืนระบบ รวมถึงทบทวนและปรับปรุงให้มีประสิทธิภาพและประสิทธิผลอยู่เสมอ
4. ดำเนินการอบรมบุคลากรที่เกี่ยวข้อง เพื่อสร้างความเข้าใจเกี่ยวกับแผนบริหารจัดการความต่อเนื่องทางธุรกิจด้านเทคโนโลยีสารสนเทศ
5. เข้าร่วมการทดสอบแผนบริหารจัดการความต่อเนื่องทางธุรกิจด้านเทคโนโลยีสารสนเทศ และรายงานผลการทดสอบต่อคณะกรรมการ
6. จัดทำแผนป้องกัน และแก้ไขปัญหาที่อาจเกิดขึ้นในการดำเนินงานของคณะทำงานบริหารจัดการความต่อเนื่องทางธุรกิจด้านเทคโนโลยีสารสนเทศ
7. ดำเนินการรวบรวมแผนป้องกันและแก้ไขปัญหา รวมถึงติดตามผลการดำเนินงานที่เกี่ยวข้อง

8. รายงานผลการดำเนินงานต่อคณะกรรมการบริหารจัดการความมั่นคงปลอดภัยข้อมูลสารสนเทศอย่างน้อยปีละ 1 ครั้ง
9. ปฏิบัติงานอื่นใดตามที่คณะกรรมการบริหารจัดการความมั่นคงปลอดภัยข้อมูลสารสนเทศมอบหมายรายละเอียดของแต่ละหน้าที่และความรับผิดชอบสามารถดูได้จากเอกสาร ISMS-1PC-005 (BCMS Framework)

10.7 คณะทำงานด้านการบริหารจัดการเหตุการณ์ละเมิดความมั่นคงปลอดภัยสารสนเทศและปฏิบัติการระบบสารสนเทศ

โดยมีความรับผิดชอบ ดังต่อไปนี้

1. ดำเนินการตามแนวนโยบายภายใต้ระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศของห้องคอมพิวเตอร์กลาง (Data Center)
2. ดำเนินการตามขั้นตอนปฏิบัติ (Procedure) ภายใต้ระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศของห้องคอมพิวเตอร์กลาง (Data Center) อย่างเหมาะสมและมีประสิทธิภาพ
3. ประเมินความเสี่ยงของสินทรัพย์สารสนเทศตามวิธีการบริหารจัดการความเสี่ยง (Risk Management Methodology) ในส่วนที่เกี่ยวข้องกับการบริหารจัดการเหตุการณ์ละเมิดความมั่นคงปลอดภัยสารสนเทศและปฏิบัติการระบบสารสนเทศ (Service Operation)
4. ดำเนินการตามแผนการสื่อสารภายใต้ระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศของห้องคอมพิวเตอร์กลาง (Data Center) ในส่วนที่เกี่ยวข้องกับการบริหารจัดการเหตุการณ์ละเมิดความมั่นคงปลอดภัยสารสนเทศและปฏิบัติการระบบสารสนเทศ (Service Operation)
5. รายงานและวิเคราะห์เหตุการณ์ละเมิดความมั่นคงปลอดภัยสารสนเทศ (Incident) ต่อผู้แทนคณะกรรมการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศอย่างน้อยเดือนละ 1 ครั้ง
6. จัดอบรมและสร้างความตระหนักด้านการรักษาความมั่นคงปลอดภัยสารสนเทศให้แก่เจ้าหน้าที่ที่เกี่ยวข้องในส่วนที่เกี่ยวข้องกับการบริหารจัดการเหตุการณ์ละเมิดความมั่นคงปลอดภัยสารสนเทศและปฏิบัติการระบบสารสนเทศ (Service Operation)
7. ให้คำแนะนำและชี้แจงเจ้าหน้าที่และบุคคลที่เกี่ยวข้องในการปฏิบัติให้เป็นไปตามมาตรฐานระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ (มาตรฐาน ISO/IEC 27001:2022) ในส่วนที่เกี่ยวข้องกับการบริหารจัดการเหตุการณ์ละเมิดความมั่นคงปลอดภัยสารสนเทศและปฏิบัติการระบบสารสนเทศ (Service Operation)

8. ประสานงานกับคณะทำงานและหน่วยงานที่เกี่ยวข้องเพื่อดำเนินการให้เป็นไปตามที่กำหนดไว้ในขั้นตอนปฏิบัติ (Procedure) ภายใต้ระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศของห้องคอมพิวเตอร์กลาง (Data Center)
9. จัดทำ ติดตาม และตรวจสอบผลการดำเนินการตามตัวชี้วัดประสิทธิภาพของระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศในส่วนที่เกี่ยวข้องกับการบริหารจัดการเหตุการณ์ละเมิดความมั่นคงปลอดภัยสารสนเทศและปฏิบัติการระบบสารสนเทศ (Service Operation)
10. เชิญบุคคลที่เกี่ยวข้องมาให้ข้อมูล ข้อเท็จจริง และข้อเสนอแนะ รวมทั้งจัดส่งเอกสารหลักฐานที่เกี่ยวข้อง เพื่อประกอบการพิจารณาของคณะทำงานด้านการบริหารจัดการเหตุการณ์ละเมิดความมั่นคงปลอดภัยสารสนเทศและปฏิบัติการระบบสารสนเทศ (Service Operation)
11. รายงานผลการดำเนินงานต่อผู้แทนคณะกรรมการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศอย่างน้อยปีละ 1 ครั้ง
12. ปฏิบัติงานอื่นใดตามที่ผู้แทนคณะกรรมการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศมอบหมาย

10.8 เจ้าของบริการ (Service Owner)

เจ้าของบริการ มีหน้าที่บริหารจัดการขอบเขตการให้บริการ และกำหนดข้อกำหนดด้านการบริการและข้อตกลงร่วมของระดับการให้บริการ (Service Level Agreement) กับผู้ใช้งานและผู้ให้บริการตลอดจนกำหนดนโยบายสนับสนุนด้านความมั่นคงปลอดภัยระบบสารสนเทศของการให้บริการ พร้อมทั้งตรวจทานและอนุมัติการนำไปปฏิบัติใช้ โดยมีส่วนร่วมในการสนับสนุนทรัพยากรที่จำเป็นเพื่อใช้ในการบริหารจัดการระบบสารสนเทศ เพื่อให้การบริการดำเนินไปอย่างมีประสิทธิภาพ รวมถึงปฏิบัติหน้าที่ในฐานะผู้แทนกรรมการบริหารจัดการความมั่นคงปลอดภัยข้อมูลสารสนเทศ

10.9 เจ้าของระบบ (System Owner)

เจ้าของระบบ คือ บุคคลซึ่งได้รับมอบหมายจากเจ้าของบริการ (Service Owner) ให้จัดการข้อมูลสารสนเทศในระบบงานของตนเอง โดยเจ้าของระบบสารสนเทศจะต้องเป็นผู้ร่วมกำหนดนโยบายสนับสนุนด้านความมั่นคงปลอดภัยระบบสารสนเทศของการให้บริการ ตลอดจนตรวจทานและรับรองสิทธิการเข้าใช้ระบบงานตามขอบเขตที่รับผิดชอบให้เหมาะสมกับระดับชั้นความลับของข้อมูล

10.10 ผู้ดูแลระบบ (Custodian)

ผู้ดูแลระบบ คือ บุคคลซึ่งได้รับมอบหมายให้บริหารจัดการระบบสารสนเทศจากเจ้าของระบบ (System Owner) โดยจะต้องปฏิบัติตามนโยบายด้านความมั่นคงปลอดภัยระบบสารสนเทศของการให้บริการ ข้อตกลงร่วมของระดับการให้บริการ (Service Level Agreement) และขั้นตอนการปฏิบัติงานด้านการรักษาความมั่นคง

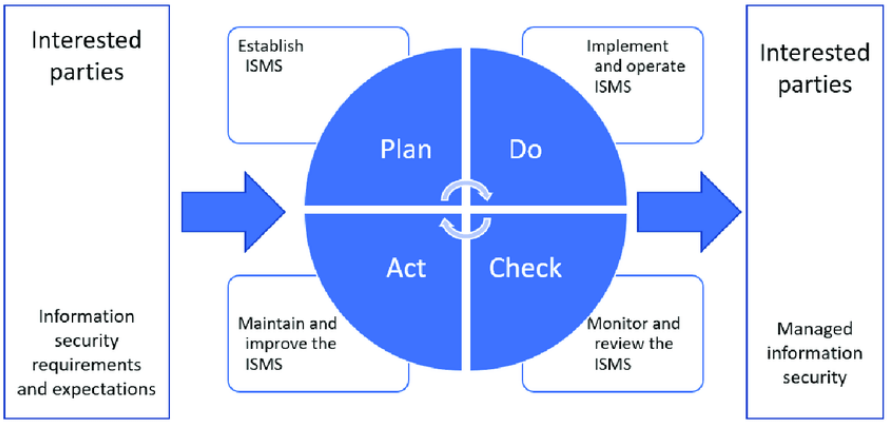
ปลอดภัยที่เจ้าของบริการกำหนดไว้ และดูแลให้ระบบสารสนเทศดังกล่าวสามารถให้บริการได้สอดคล้องกับข้อกำหนดในนโยบายด้านความมั่นคงปลอดภัยด้วย ทั้งนี้ การเพิ่มหรือเพิกถอนสิทธิในการเข้าถึงระบบใด ๆ ให้ปฏิบัติตามเอกสารกระบวนการที่เจ้าของบริการกำหนดอย่างเคร่งครัด ตลอดจนทบทวนความเหมาะสมของมาตรการที่นำมาใช้ พร้อมทั้งรายงานผลการดำเนินงานให้เจ้าของระบบ (System Owner) อย่างน้อยปีละ 1 ครั้ง

10.11 ผู้ใช้งานหรือผู้ใช้ (User)

ผู้ใช้งาน หรือผู้ใช้ ได้แก่ บุคคล (หรือบางครั้งอาจหมายถึงระบบสารสนเทศหรือกระบวนการ) ที่ได้รับอนุญาตให้สามารถเข้าถึงข้อมูลสารสนเทศได้ตามกระบวนการหรือข้อบังคับของเจ้าของระบบเอง อย่างไรก็ตามผู้ใช้งานจะต้องปกป้องข้อมูลภายใต้การควบคุมของผู้ดูแลระบบ และจะต้องปฏิบัติตามข้อกำหนดในนโยบาย มาตรฐาน และแนวทางการดำเนินงานที่เกี่ยวข้อง ทั้งนี้ ผู้ใช้งานจะต้องรับผิดชอบการดำเนินการใด ๆ ที่เกี่ยวข้องกับการใช้งานข้อมูลสารสนเทศ หากทราบหรือสงสัยว่ามีการละเมิดนโยบายความมั่นคงปลอดภัยสารสนเทศ จะต้องรายงานต่อผู้บังคับบัญชาหรือผู้แทนกรรมการบริหารจัดการความมั่นคงปลอดภัยข้อมูลสารสนเทศ (ISMR) โดยทันที

11. กรอบการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ

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

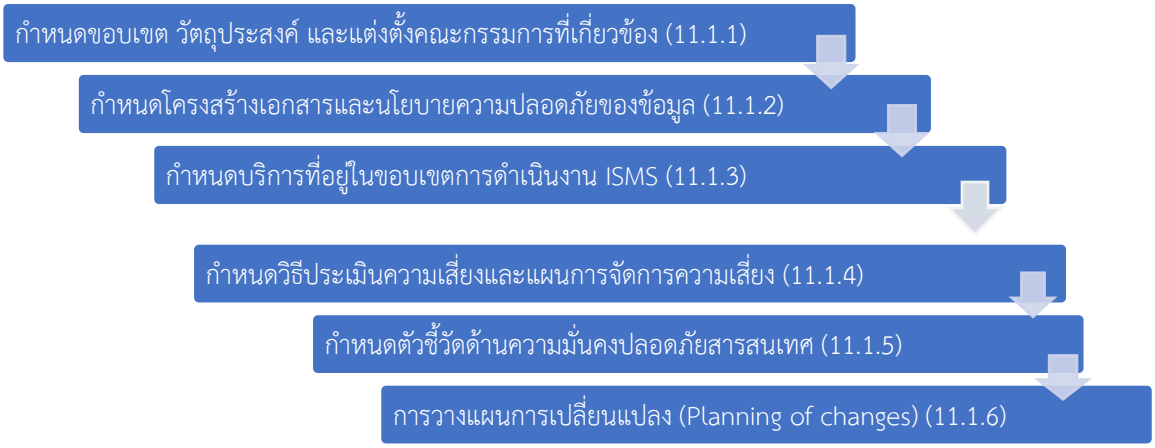


รูปที่ 1 : แสดงโมเดล Plan-Do-Check-Act (PDCA)[1]

[1] MBSEsec: Model-Based Systems Engineering Method for Creating Secure Systems - Scientific Figure on ResearchGate. Available from: https://www.researchgate.net/figure/Plan-Do-Check-Act-PDCA-model-applied-to-information-security-management-system-ISMS_fig1_340566504 [accessed 23 Oct 2024]

11.1 กิจกรรมวางแผน (Plan)

รายละเอียดของกิจกรรมนี้ ประกอบไปด้วยกระบวนการ 5 ขั้นตอน ดังนี้



รูปที่ 2 : แสดงรายละเอียดของกิจกรรมวางแผน

11.1.1 กำหนดขอบเขต วัตถุประสงค์ และแต่งตั้งคณะกรรมการที่เกี่ยวข้อง

- การกำหนดขอบเขตของการนำระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ (ISMS) รวมถึงการกำหนดพันธกิจ วิสัยทัศน์ ตลอดจนวัตถุประสงค์ทางด้านความปลอดภัยสารสนเทศ ให้สอดคล้องกับเป้าหมายและวัตถุประสงค์ของสำนักคอมพิวเตอร์มหาวิทยาลัยศรีนครินทรวิโรฒ
- การกำหนดปัจจัยและปัญหาที่นำมาสู่การดำเนินกิจกรรมในระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศของสำนักคอมพิวเตอร์ มหาวิทยาลัยศรีนครินทรวิโรฒ ตลอดจนผู้ที่เกี่ยวข้องและความไม่เป็นอิสระต่อหน่วยงานต่าง ๆ
- แต่งตั้งคณะกรรมการทางด้าน ISMS เพื่อร่วมขับเคลื่อนระบบ ISMS ภายใต้ขอบเขตที่กำหนดไว้
- จัดทำเอกสารนโยบายระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ ซึ่งจะกำหนดพันธกิจ วิสัยทัศน์ วัตถุประสงค์ ตลอดจนหน้าที่ความรับผิดชอบของคณะกรรมการที่เกี่ยวข้องกับการดำเนินการระบบ ISMS และเอกสารขอบเขตระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ

11.1.2 กำหนดโครงสร้างเอกสารและนโยบายความปลอดภัยของข้อมูล

- กำหนดโครงสร้างเอกสารระบบ ISMS เพื่อใช้ควบคุมเอกสารต่าง ๆ ที่อยู่ในระบบและแสดงถึงลำดับความสำคัญของเอกสารในแต่ละระดับ สำหรับรายละเอียดในส่วนนี้จะถูกอธิบายไว้ในระเบียบขั้นตอนการควบคุม เอกสาร (Document Control Procedure)

- นโยบายระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ (ISMS Policy) จะประกอบไปด้วยหลักการด้านความมั่นคงปลอดภัยสารสนเทศซึ่งจะต้องได้รับการทบทวนและอนุมัติโดยผู้มีอำนาจ (Top Management)

11.1.3 กำหนดขอบเขตการดำเนินงาน ISMS

- กำหนดบริการที่ต้องการจะรับการตรวจสอบเพื่อขอรับใบรับรอง (Certificate) โดยต้องอยู่ในขอบเขตที่กำหนดไว้
- การกำหนดบริการและระบบสารสนเทศ รวมทั้งรายการสินทรัพย์สารสนเทศภายในขอบเขตของการดำเนินงาน จะพิจารณาตามประเด็นบริการด้านเทคโนโลยีสารสนเทศหลักที่มีผลต่อภารกิจของสำนักคอมพิวเตอร์ มหาวิทยาลัยศรีนครินทรวิโรฒ ข้อมูลดังกล่าวข้างต้น จะถูกจัดเก็บไว้ในรายการบัญชีสินทรัพย์

11.1.4 กำหนดวิธีประเมินความเสี่ยงและการจัดการความเสี่ยง

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

11.1.5 กำหนดตัวชี้วัด

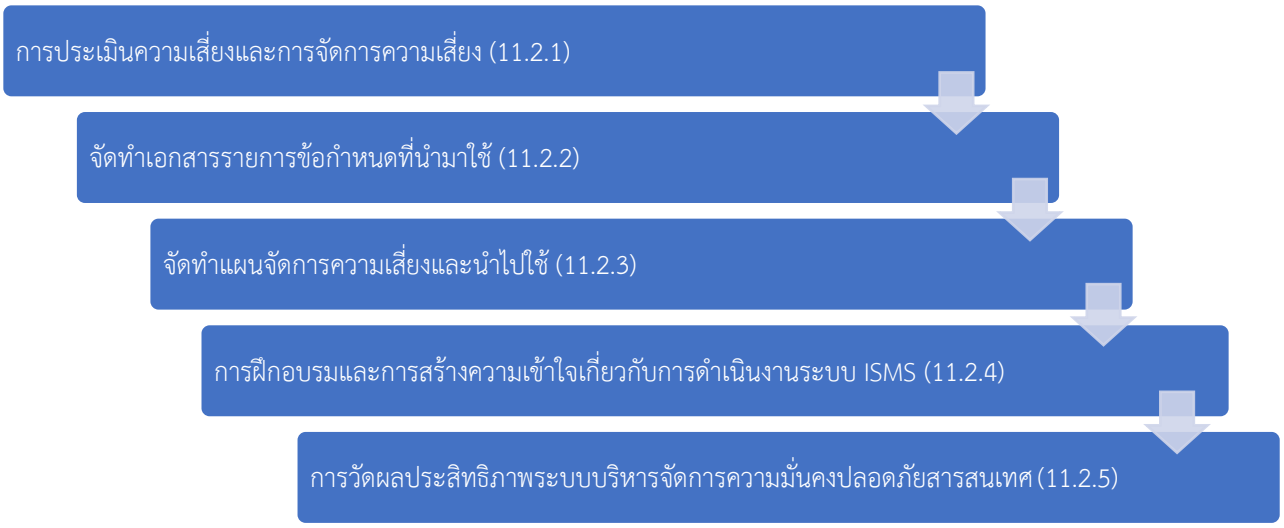
- ต้องมีการกำหนดตัวชี้วัดเพื่อประเมินประสิทธิภาพของมาตรการต่าง ๆ ที่นำมาใช้
- ตัวชี้วัดจะต้องเป็นการวัดผลเชิงปริมาณ โดยตัวชี้วัดดังกล่าวจะต้องมีองค์ประกอบดังต่อไปนี้
    - เป้าหมายการนำไปใช้งาน (Objective of The Metrics)
    - การวัดและวิเคราะห์ผล (Measurement of The Metrics)
    - วัตถุประสงค์การนำไปใช้ (Purpose of Metrics)
    - ความถี่ในการเก็บข้อมูล (Frequency)
    - การคำนวณค่าของตัวชี้วัด (Process Method)
    - ทรัพยากรที่ต้องใช้ในการดำเนินการวัดผล (Resource)
- ต้องจัดทำเอกสารอ้างอิงเพื่อสนับสนุนการเก็บรวบรวมและวิเคราะห์ในเมตริก ตัวชี้วัดตัวเดียวกันอาจนำไปใช้สำหรับมาตรการอื่น ๆ ได้ หากข้อมูลที่ได้จากตัวชี้วัดดังกล่าวสามารถนำไปใช้วัดผลวัตถุประสงค์ของมาตรการดังกล่าวได้

11.1.6 การวางแผนการเปลี่ยนแปลง (Planning of changes)

การวางแผนการเปลี่ยนแปลง ISMS เป็นกระบวนการที่สำคัญในการรักษาความมั่นคงปลอดภัยสารสนเทศ ก่อนดำเนินการเปลี่ยนแปลง จะต้องมีการกำหนดขอบเขตของการเปลี่ยนแปลงอย่างชัดเจน พร้อมทั้งประเมินผลกระทบที่อาจเกิดขึ้นต่อระบบ ISMS จากนั้นจึงพัฒนามาตรการแก้ไขและวางแผนการดำเนินงานอย่างเป็นระบบ โดย ISMR จะมีหน้าที่ในการติดตาม ประชุมประเมินผลการดำเนินงาน และรายงานผลต่อ Steering Committee อย่างน้อยปีละ 1 ครั้ง เพื่อให้มั่นใจว่าการเปลี่ยนแปลงเป็นไปตามแผนที่กำหนด และสอดคล้องกับมาตรฐานความมั่นคงปลอดภัยสารสนเทศ

11.2 กิจกรรมดำเนินการ (Do)

รายละเอียดของขั้นตอนดำเนินการ (Do) ของกรอบวิธีดำเนินการระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ (ISMS Framework) เป็นดังต่อไปนี้



รูปที่ 3 : แสดงรายละเอียดของกิจกรรมดำเนินการ

11.2.1 การประเมินความเสี่ยงและการจัดการความเสี่ยง

- ผู้ดูแลระบบและเจ้าของที่เกี่ยวข้องกับระบบสารสนเทศที่อยู่ในขอบเขตการดำเนินงานระบบ ISMS จะทำการตรวจสอบสินทรัพย์ของตนเอง ประเมินผลกระทบ และความเสี่ยงของสินทรัพย์ตามแนวทางการประเมินความเสี่ยง
- กำหนดระดับความเสี่ยงที่ยอมรับได้ (Risk Appetite Statement : RAS) โดยเปรียบเทียบกับความเสี่ยงในปัจจุบัน และดำเนินการลดความเสี่ยงสำหรับสินทรัพย์ที่มีค่าความเสี่ยงมากเกินกว่าค่าที่ยอมรับได้

11.2.2 จัดทำเอกสารรายการข้อกำหนดที่นำมาใช้ (Statement of Applicability)

- รายการข้อกำหนดที่นำมาใช้ (SOA) จะเป็นเอกสารที่ระบุถึงวัตถุประสงค์ในการควบคุม (Control Objective) และมาตรการควบคุม (Controls) ด้านความมั่นคงปลอดภัยที่สำนักคอมพิวเตอร์ มหาวิทยาลัยศรีนครินทรวิโรฒ 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

11.2.3 จัดทำแผนการจัดการความเสี่ยงและนำไปใช้

- จัดทำแผนการจัดการความเสี่ยงตามผลที่ได้รับจากการประเมินความเสี่ยง และติดตามตรวจสอบการดำเนินงาน การประเมินความเสี่ยงคงเหลือในระบบ

11.2.4 การฝึกอบรมและการสร้างความเข้าใจเกี่ยวกับการดำเนินงานระบบ ISMS

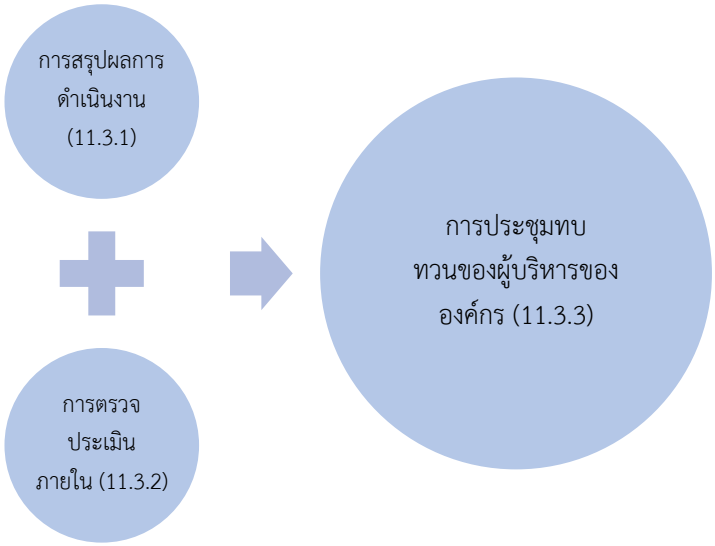
- บุคลากรที่เกี่ยวข้องกับการดำเนินงานระบบ ISMS จะต้องได้รับการอบรมเกี่ยวกับการปฏิบัติตามกระบวนการต่าง ๆ ที่มีในระบบ
- บุคลากรควรได้รับการฝึกอบรม 2 ประเภท (ตามความเหมาะสม) ดังนี้
  - การอบรมทั่วไป เพื่อให้เกิดความตระหนักเกี่ยวกับมาตรการที่สำนักคอมพิวเตอร์ มหาวิทยาลัยศรีนครินทรวิโรฒ นำมาใช้ รวมถึงระดับชั้นความลับและกระบวนการในการจัดการข้อมูล
  - การฝึกอบรมเฉพาะทาง เพื่อช่วยเพิ่มความชำนาญในการปฏิบัติงาน

11.2.5 การวัดผลประสิทธิภาพระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ

- บันทึกและจัดเก็บเอกสารต่าง ๆ สามารถใช้เป็นหลักฐานเพื่อแสดงว่ามาตรการที่ได้นำมาใช้นั้นมีการนำไปใช้งานจริงและสอดคล้องกับข้อกำหนด
- บันทึกดังกล่าวจะต้องได้รับการควบคุมตามระเบียบการปฏิบัติ เรื่องขั้นตอนการควบคุมเอกสารและบันทึกการใช้งาน (Record Control Procedure)

11.3 กิจกรรมตรวจสอบ (Check)

รายละเอียดของขั้นตอนตรวจสอบตามกรอบวิธีดำเนินการระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ (ISMS Framework) มีดังนี้



รูปที่ 4 : แสดงรายละเอียดของกิจกรรมตรวจสอบ

11.3.1 การสรุปผลการดำเนินงาน

คณะทำงานปฏิบัติการงานบริหารจัดการความมั่นคงปลอดภัยข้อมูลสารสนเทศ ต้องตรวจสอบและสรุปผลการดำเนินงานด้านความมั่นคงปลอดภัยสารสนเทศ เพื่อรายงานแก่ผู้บริหารขององค์กร โดยการสรุปผลและหลักฐานหรือเหตุการณ์ต่าง ๆ ที่มีนัยสำคัญต่อประสิทธิภาพของระบบและการพัฒนาปรับปรุงอย่างต่อเนื่อง เช่น

- ความคิดเห็นและผลตอบรับ (Feedback) จากผู้ปฏิบัติงานในทุกระดับชั้น
- ผลการประเมินความเสี่ยงและการบริหารจัดการความเสี่ยง ตลอดจนความเสี่ยงคงเหลือในระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ (Risk Management Result)
- ผลของการวัดประเมินประสิทธิภาพของระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ (ISMS Measurement Result)
- เหตุการณ์สำคัญที่มีผลกระทบต่อระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ (Event)
- โอกาสในการพัฒนาปรับปรุงอย่างต่อเนื่อง (Opportunity for Improvement)

11.3.2 การตรวจประเมินภายใน (Internal Audit)

- คณะตรวจประเมินภายใน ดำเนินการตรวจสอบตามความสอดคล้อง ดังต่อไปนี้
  - ต้องดำเนินการตรวจประเมินภายในตามรอบระยะเวลาที่กำหนด

- ต้องสอดคล้องต่อนโยบายของสำนักคอมพิวเตอร์มหาวิทยาลัยศรีนครินทรวิโรฒ
- ต้องสอดคล้องต่อข้อกำหนดของมาตรฐานสากล ISO/IEC 27001:2022
- ต้องสอดคล้องด้านกฎหมายและข้อบังคับทางสัญญาจากหน่วยงานที่เกี่ยวข้องกับระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ
- ต้องนำไปปฏิบัติและรักษาให้คงไว้อย่างมีประสิทธิผล
- ต้องวางแผน จัดตั้ง นำไปปฏิบัติ และรักษาให้คงไว้ของโปรแกรมการตรวจประเมิน (Audit Programme) ซึ่งรวมถึงความถี่ วิธีการ หน้าที่ความรับผิดชอบ ข้อกำหนดของการวางแผน และการรายงาน
- เมื่อจัดตั้งโปรแกรมการตรวจประเมินภายใน องค์กรต้องพิจารณาถึงความสำคัญของกระบวนการที่เกี่ยวข้องและผลการตรวจประเมินครั้งก่อน
- ต้องกำหนดเกณฑ์การตรวจประเมิน และขอบเขตสำหรับการตรวจประเมินแต่ละครั้ง
- ต้องคัดเลือกผู้ตรวจประเมินและดำเนินการตรวจประเมิน เพื่อให้มั่นใจได้ถึงความเป็นกลาง และความเป็นธรรมของกระบวนการตรวจประเมิน
- ผลที่ได้จากการตรวจประเมินได้นำไปรายงานต่อผู้บริหารที่เกี่ยวข้อง
- เอกสารสารสนเทศจะต้องจัดทำเพื่อเป็นหลักฐานของการดำเนินการตามโปรแกรมการตรวจประเมินและผลการตรวจประเมิน
- ผลการตรวจสอบจะต้องถูกนำส่งผู้บริหารขององค์กร เพื่อนำไปพิจารณาแนวทางในการพัฒนาและปรุงปรุงต่อไป

11.3.3 การประชุมทบทวนของผู้บริหารขององค์กร

- การทบทวนการดำเนินงานระบบ ISMS โดยผู้บริหารขององค์กร จะต้องจัดขึ้นอย่างน้อย 1 ครั้งต่อปี โดยผลของการทบทวนต้องมีการจัดเก็บเป็นลายลักษณ์อักษร และแสดงถึง
  - ผลจากการทำ Management Review ที่ผ่านมาและการแก้ไขตามคำแนะนำของผู้บริหารขององค์กร
  - การเปลี่ยนแปลงของประเด็นภายในและภายนอกที่เกี่ยวข้องกับระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ
  - การเปลี่ยนแปลงความต้องการและความคาดหวังของผู้มีส่วนได้ส่วนเสียที่เกี่ยวข้องกับระบบการจัดการความมั่นคงปลอดภัยสารสนเทศ
  - ผลตอบกลับจากประสิทธิภาพของความมั่นคงปลอดภัยสารสนเทศ รวมถึงแนวโน้ม

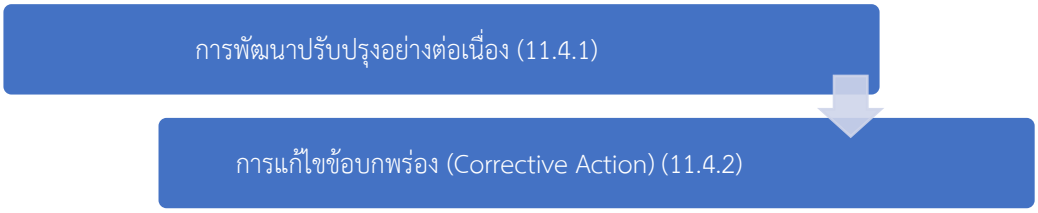
ความไม่สอดคล้อง และการดำเนินการแก้ไข

- ผลการวัดประสิทธิภาพของระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ
- ผลลัพธ์จากการตรวจประเมิน
- ความสำเร็จของวัตถุประสงค์ความมั่นคงปลอดภัยสารสนเทศ

- เหตุการณ์หรือการละเมิดความมั่นคงปลอดภัยสารสนเทศที่เกิดขึ้น (Incident)
- ผลตอบกลับจากผู้มีส่วนได้ส่วนเสีย
- ผลลัพธ์จากการประเมินความเสี่ยง และสถานะของแผนการจัดการความเสี่ยง
- โอกาสสำหรับการปรับปรุงพัฒนาอย่างต่อเนื่อง
- ผลลัพธ์การทบทวนของฝ่ายบริหาร ต้องรวมถึง การตัดสินใจที่เกี่ยวกับการปรับปรุงพัฒนาอย่างต่อเนื่อง และความจำเป็นใด ๆ เพื่อการเปลี่ยนแปลงต่อระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ
- เอกสารสารสนเทศจะต้องจัดทำเพื่อเป็นหลักฐานแสดงผลลัพธ์การทบทวนของฝ่ายบริหาร

11.4 กิจกรรมปรับปรุง (Act)

รายละเอียดของขั้นตอนการปรับปรุงวิธีดำเนินการระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ (ISMS Framework) มีดังนี้



รูปที่ 5 : แสดงรายละเอียดของกิจกรรมปรับปรุง

11.4.1 การพัฒนาปรับปรุงอย่างต่อเนื่อง

สำนักคอมพิวเตอร์ มหาวิทยาลัยศรีนครินทรวิโรฒต้องดำเนินกิจกรรมการพัฒนาปรับปรุงระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ ตามแนวทางที่ได้มีการกำหนดขึ้นอย่างต่อเนื่อง

11.4.2 การแก้ไขข้อบกพร่อง

ปัญหาหรือความไม่สอดคล้องต่าง ๆ ต้องได้รับการแก้ไขและติดตามผลผ่านกระบวนการทำCorrective Action. เมื่อความไม่สอดคล้องเกิดขึ้น องค์กรต้องดำเนินการ ดังนี้

- ตอบสนองต่อความไม่สอดคล้อง และตามความเหมาะสม

- ดำเนินการเพื่อควบคุมและแก้ไข
- รับมือกับผลกระทบที่ตามมา

- ประเมินความจำเป็นสำหรับดำเนินการขจัดสาเหตุของความไม่สอดคล้อง เพื่อไม่ให้ความไม่สอดคล้องเกิดขึ้นซ้ำ หรือไม่เกิดขึ้นที่อื่น ๆ โดย
  - ทบทวนความไม่สอดคล้อง
  - ระบุสาเหตุของความไม่สอดคล้อง
  - ระบุความไม่สอดคล้องที่คล้ายกันมีอยู่ หรือสามารถมีโอกาสเกิดขึ้นได้
- ดำเนินการปฏิบัติที่จำเป็น
- ทบทวนประสิทธิผลของการปฏิบัติการแก้ไข
- ทำการเปลี่ยนแปลงระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ ถ้าจำเป็น
- การปฏิบัติการแก้ไขต้องเหมาะสมต่อผลกระทบของความไม่สอดคล้องที่พบ
- เอกสารสารสนเทศจะต้องจัดทำเพื่อเป็นหลักฐานแสดง ลักษณะของความไม่สอดคล้องและการปฏิบัติใด ๆ ที่ได้ดำเนินการ และผลลัพธ์ของการปฏิบัติการแก้ไข

11.5 การสนับสนุน (Support)

กิจกรรมสนับสนุนถือว่ามีบทบาทเพิ่มเติมในวงจร P-D-C-A เพราะเป็นกิจกรรมที่เกิดขึ้นตลอดการดำเนินกิจกรรมในระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ เช่น

11.5.1 การควบคุมเอกสารและหลักฐานการดำเนินกิจกรรม

- สำนักคอมพิวเตอร์ มหาวิทยาลัยศรีนครินทรวิโรฒ ต้องควบคุมหลักฐานการดำเนินกิจกรรมเพื่อใช้ยืนยันความสอดคล้องและแนวทางการปฏิบัติ ตามกระบวนการควบคุมเอกสารที่ได้มีการจัดทำขึ้น และสอดคล้องกับข้อกำหนดของมาตรฐาน และหมายรวมถึงการควบคุมเอกสารภายนอกที่เกี่ยวข้อง
- หลักฐานและเอกสารในทุกรูปแบบ ต้องมีการจัดเก็บและควบคุมตามระดับชั้นความลับและระยะเวลาการจัดเก็บที่เหมาะสม

11.5.2 การส่งเสริมศักยภาพและทักษะความสามารถ

- สำนักคอมพิวเตอร์ มหาวิทยาลัยศรีนครินทรวิโรฒ ต้องพิจารณาโอกาสในการส่งเสริมศักยภาพของบุคลากร ความพร้อมทางด้านทักษะในการดำเนินกิจกรรมให้บรรลุวัตถุประสงค์และความคาดหวังในหน้าที่ความรับผิดชอบ

12. กิจกรรมที่เกี่ยวข้องในขอบเขต

ลำดับที่	กิจกรรมในขอบเขต
1	การบริหารจัดการสิทธิ
2	การบริหารจัดการเครือข่าย
3	การป้องกันโปรแกรมไม่ประสงค์ดี
4	การเฝ้าระวังระบบ และการบริหารจัดการทรัพยากรคอมพิวเตอร์
5	การบำรุงรักษาระบบและอุปกรณ์
6	การสำรองข้อมูล
7	การควบคุมการเปลี่ยนแปลง
8	การบริหารจัดการเหตุขัดข้อง
9	การเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์