คู่มือระบบบริหารความมั่นคงปลอดภัยสารสนเทศ
ISMS Manual

คณะแพทยศาสตร์ มหาวิทยาลัยเชียงใหม่

รหัสเอกสาร : ISMS-PL-I-006
ฉบับที่ : 2.1
ประเภทเอกสาร : เอกสารภายใน

สารบัญ

การควบคุมเอกสาร

การอนุมัติใช้เอกสาร

เอกสารนี้ผ่านการทบทวนและอนุมัติโดย:

จัดเตรียมเอกสารโดย	ทบทวนเอกสารโดย	อนุมัติเอกสารโดย
(นางสาวอลิศา นิ่มวรพันธุ์) คณะทำงานระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ	(นางอัจฉราภรณ์ อังศุรัตนเวช) ผู้บริหารระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ	(ศาสตราจารย์ (เชี่ยวชาญพิเศษ) นายแพทย์บรรณกิจ โลจนาภิวัฒน์) ประธานกรรมการอำนวยการระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ
วันที่ 17 กุมภาพันธ์ 2566	วันที่ 20 กุมภาพันธ์ 2566	วันที่ 20 กุมภาพันธ์ 2566

ประวัติการปรับปรุงเอกสาร

ตารางบันทึกประวัติการปรับปรุงเอกสาร:

ฉบับที่	วันที่	รายละเอียดการปรับปรุงเอกสาร	อนุมัติโดย
1.0	9 กันยายน 2565	เริ่มต้นใช้งานเอกสาร	ศ.(เชี่ยวชาญพิเศษ) นพ. บรรณกิจ โลจนาภิวัฒน์
2.0	26 มกราคม 2566	เพิ่มระดับชั้นความลับในรหัสเอกสาร	ศ.(เชี่ยวชาญพิเศษ) นพ. บรรณกิจ โลจนาภิวัฒน์
2.1	17 กุมภาพันธ์ 2566	เพิ่มความคาดหวังของผู้ให้บริการภายนอก แก้ไขสิ่งที่ครอบคลุมในการขอรับรอง	ศ.(เชี่ยวชาญพิเศษ) นพ. บรรณกิจ โลจนาภิวัฒน์

คู่มือการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ (ISMS Manual)

1. วัตถุประสงค์ของระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ

1. เพื่อปกป้องข้อมูลและระบบสารสนเทศให้มีความมั่นคงปลอดภัย และสร้างความเชื่อมั่นให้แก่ผู้ที่เกี่ยวข้อง รวมถึงการให้บริการอย่างต่อเนื่อง
2. เพื่อรักษาความมั่นความมั่นคงปลอดภัยของข้อมูลในระบบงานให้ได้รับการปกป้องจากการเข้าถึงโดยไม่ได้รับอนุญาต
3. ข้อมูลสารสนเทศที่สำคัญ และเป็นความลับได้รับการดูแลอย่างเหมาะสม
4. เพื่อให้การบริการมีการรักษาความมั่นคงปลอดภัยตามมาตรฐานสากล และเป็นบริการที่ได้รับการยอมรับจากผู้ใช้บริการ
5. คณะแพทยศาสตร์ มหาวิทยาลัยเชียงใหม่ ได้การรับรองตามมาตรฐาน ISO/IEC 27001:2013

2. บริบทภายในและภายนอกขององค์กร

เพื่อกำหนดขอบข่ายของระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ ทางคณะฯ ได้จัดให้มีการวิเคราะห์บริบทภายในและภายนอก รวมถึงความคาดหวังของผู้ที่เกี่ยวข้อง ดังต่อไปนี้

2.1 บริบทภายใน

หมายถึง ปัจจัยภายในของคณะฯ ที่เป็นเหตุผลในการพิจารณาขอบข่ายของระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ (Information Security Management System: ISMS)

ภาพรวมการดำเนินงาน

คณะแพทยศาสตร์ มหาวิทยาลัยเชียงใหม่ การดำเนินงานการให้บริการในหลายด้าน ได้แก่

บริการทางด้านการศึกษา

ให้บริการหลักสูตรแพทยศาสตรบัณฑิต หลักสูตรบัณฑิตศึกษาและหลักสูตรฝึกอบรมแพทย์ประจำบ้านสาขาต่าง ๆ ภายใต้การกำกับดูแลและรับรองคุณภาพโดย WFME, สำนักงานคณะกรรมการการอุดมศึกษา (สกอ.) แพทยสภาและราชวิทยาลัยที่เกี่ยวข้อง

บริการทางด้านวิจัย

คณะแพทยศาสตร์ มหาวิทยาลัยเชียงใหม่ ดำเนินการวิจัยด้านสุขภาพเพื่อความเป็นเลิศทางวิชาการใช้พัฒนาและสร้างองค์ความรู้สนับสนุนการเรียนรู้ของผู้เรียนและเป็นประโยชน์ในการพัฒนาสังคม

บริการทางการแพทย์

ให้บริการรักษาพยาบาลแก่ผู้ป่วยที่ได้มาตรฐานสากล เพื่อใช้เป็นแหล่งสนับสนุนการจัดการเรียนการสอนให้แก่ผู้เรียนและสนับสนุนการวิจัย ผ่านการดำเนินการของโรงพยาบาลมหาราชนครเชียงใหม่ ซึ่งเป็นโรงพยาบาลตติยภูมิ ขนาด 1,400 เตียง จัดเป็นโรงพยาบาลที่มีขนาดใหญ่ที่สุดในภาคเหนือ

วิสัยทัศน์

โรงเรียนแพทย์ในดวงใจ เพื่อยกระดับสุขภาพและสุขภาวะที่ยั่งยืนของมนุษยชาติ

พันธกิจ

ด้านการศึกษา ผลิตบัณฑิตที่มีคุณภาพ คุณธรรม เป็นสากล
ด้านการวิจัย สร้างสรรค์งานวิจัยและนวัตกรรมระดับสากล เพื่อชี้นำด้านสุขภาพ
ด้านการบริการ ให้บริการสุขภาพที่ได้มาตรฐานระดับสากล

ผู้บริหาร

1. ต้องการให้มีการกำกับดูแลตามนโยบายของคณะฯ เช่น ปฏิบัติตามนโยบายเทคโนโลยีสารสนเทศ, การบริหารความเสี่ยงของคณะฯ เป็นต้น
2. เพื่อให้มีความสอดคล้องกับการดำเนินกลยุทธ์ของคณะฯ เพื่อทำให้คณะฯ มีความน่าเชื่อถือ มีประสิทธิภาพ ประสิทธิผลในการดำเนินงาน ตอบสนองความต้องการและความคาดหวังของผู้บริหารและผู้ที่มีส่วนได้เสีย
3. ต้องการจัดการทรัพยากรที่มีอยู่ในคณะฯ อย่างมีประสิทธิภาพ
4. ต้องการสร้างกระบวนการที่มีประสิทธิภาพในการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศของคณะฯ และวางรากฐานในการประยุกต์ใช้กระบวนการบริหารความมั่นคงปลอดภัยสารสนเทศในส่วนงานอื่นๆ ของคณะฯ
5. เพื่อให้มีระบบการจัดการความมั่นคงปลอดภัยสารสนเทศของคณะฯ ตามมาตรฐานสากล (ISO/IEC 27001:2013)

2.2 บริบทภายนอก

หมายถึง ปัจจัยภายนอกคณะฯ ที่เป็นเหตุผลในการพิจารณาขอบข่ายของระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ (Information Security Management System : ISMS) ได้แก่

1. ต้องการปกป้องภัยคุกคาม และความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศ
2. ต้องปฏิบัติตามพระราชบัญญัติ ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 และฉบับแก้ไขเพิ่มเติม (ฉบับที่ 2) พ.ศ. 2560
3. ต้องปฏิบัติตามพระราชบัญญัติ การรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ.2562
4. ต้องปฏิบัติตามพระราชบัญญัติ คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562
5. ต้องการสร้างความเชื่อมั่นให้แก่ ผู้รับบริการ และผู้ใช้งานว่า ระบบสารสนเทศของคณะฯ มีความมั่นคงปลอดภัย
6. เพื่อเตรียมความพร้อมต่อภาวะฉุกเฉินและการเกิดอุบัติการณ์ (Incident) ต่างๆ เพื่อลดความเสียหายและทำให้ องค์กร สามารถดำเนินงานได้อย่างต่อเนื่อง เช่น ระบบสารสนเทศล่ม การโจมตีผ่านทางไซเบอร์ (Cyber-attack) เป็นต้น

2.3 ความต้องการและความคาดหวังของผู้ที่เกี่ยวข้อง (Needs and expectations of interested parties)

หมายถึง ความคาดหวัง หรือความต้องการของผู้ที่มีส่วนได้ส่วนเสีย หรือผู้ที่มีหน้าที่กำกับดูแลการดำเนินงานของคณะฯ ในประเด็นที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยสารสนเทศ ได้แก่

1. **ความคาดหวังของผู้บริหาร** คือ ผู้บริหารต้องการให้มีการกำกับดูแลกิจการที่ดี มีการดำเนินการที่มีประสิทธิภาพ ประสิทธิผล มีความน่าเชื่อถือ สนับสนุนการเติบโตขององค์กร และสร้างความเชื่อมั่นให้กับผู้รับบริการ และผู้ใช้งาน
2. **ความคาดหวังของผู้รับบริการ และผู้ใช้งาน** คือ ผู้รับบริการ และผู้ใช้งานต้องการให้ข้อมูลของผู้รับบริการ และผู้ใช้งานมีความมั่นคงปลอดภัย ไม่ถูกเปิดเผย ไม่ถูกใช้งาน และ ไม่ถูกเปลี่ยนแปลงแก้ไขข้อมูลโดยไม่ได้รับอนุญาต
3. **ความคาดหวังของผู้ให้บริการภายนอก** คือ ผู้ให้บริการต้องการให้ข้อมูลที่ได้ให้บริการแก่คณะฯ มีความมั่นคงปลอดภัย ไม่ถูกเปิดเผย ไม่ถูกใช้งาน และ ไม่ถูกเปลี่ยนแปลงแก้ไขข้อมูลโดยไม่ได้รับอนุญาต รวมถึง การให้บริการในการสนับสนุนการทำงานของศูนย์คอมพิวเตอร์แม่ข่ายหลัก และ ศูนย์คอมพิวเตอร์สำรองมีความราบรื่น
4. **ต้องการปฏิบัติตามกฎหมาย ข้อบังคับ และข้อสัญญาที่เกี่ยวข้อง** เช่น
   - พระราชบัญญัติว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.2550
   - พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ ฉบับแก้ไขเพิ่มเติม (ฉบับที่ 2) พ.ศ. 2560
   - พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562
   - ประกาศกระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร เรื่อง หลักเกณฑ์การเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ของผู้ให้บริการ พ.ศ. 2550
   - กฎหมาย กฎ ระเบียบ หรือข้อบังคับที่เกี่ยวข้องของกระทรวงการอุดมศึกษา วิทยาศาสตร์ วิจัยและนวัตกรรม

3. คำจำกัดความ

1. ระบบ ISMS หมายถึง ระบบการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ (Information Security Management System: ISMS)
2. Interested parties หมายถึง ผู้เกี่ยวข้อง เช่น กลุ่ม บุคคล หรือหน่วยงานต่างๆ ที่คณะฯ ต้องให้ความสนใจ (Interested parties) จะหมายถึงกลุ่มต่างๆ ที่ได้รับผลกระทบจากคณะฯ (เหมือนกับผู้มีส่วนได้ส่วนเสีย) และมีผลกระทบต่อคณะฯ (ส่วนที่แตกต่าง) ที่จะทำให้คณะฯ ไม่สามารถบรรลุเป้าหมายของคณะฯ ซึ่งจะครอบคลุมหน่วยงานที่เกี่ยวข้องได้กว้างกว่า เช่น ผู้รับบริการ บุคลากรในคณะฯ ผู้ส่งมอบ ผู้รับจ้างช่วง หน่วยงานของรัฐทั้งระดับท้องถิ่นและระดับประเทศ ชุมชนต่างๆ เป็นต้น
3. บันทึก (Record) หมายถึง หน่วยหนึ่งของข้อมูลที่บันทึกไว้ในฐานหรือคลังข้อมูลเพื่อใช้เป็นหลักฐานในการดำเนินงานต่างๆ ของคณะฯ
4. บัญชีรายชื่อบันทึก (Record List) หมายถึง บัญชีรายชื่อข้อมูลที่บันทึกไว้ในฐานหรือคลังข้อมูลเพื่อใช้เป็นหลักฐานในการดำเนินงาน
5. Incident หมายถึง เหตุการณ์ด้านความมั่นคงปลอดภัย หรือ อุบัติการณ์ต่างๆ
6. ISMS Steering Committee หมายถึง คณะกรรมการรักษาความมั่นคงปลอดภัยสารสนเทศ
7. Information Security Management Representative (ISMR) หมายถึง ผู้บริหารระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ

8. Information Security Management Assistance (ISMA) หมายถึง ผู้ช่วยผู้บริหารระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ
9. ISMS Core Team (CT) หมายถึง คณะทำงานหลักระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ
10. ISMS Compliance Officer หมายถึง ผู้ทำหน้าที่ควบคุมให้ปฏิบัติตามกฎระเบียบข้อกำหนดของมาตรฐาน ISO 27001: 2013
11. ผู้ควบคุมเอกสาร (Document Controller) หมายถึง ผู้ทำหน้าที่ดูแลและควบคุมการใช้งานเอกสารและบันทึกต่างๆ ของระบบ ISMS ให้เป็นไปตามข้อกำหนดของมาตรฐาน ISO 27001: 2013
12. ผู้ตรวจสอบภายใน (Internal ISMS Auditor) หมายถึง ผู้ที่ได้รับมอบหมายให้ทำหน้าที่ตรวจประเมินภายในระบบ ISMS ของคณะฯ
13. Asset Owner หมายถึง เจ้าของทรัพย์สินหรือผู้ที่ได้รับมอบหมายให้มีหน้าที่รับผิดชอบในการจัดการทรัพย์สินสารสนเทศ
14. Risk Owner หมายถึง เจ้าของความเสี่ยง หรือ ผู้มีหน้าที่ความรับผิดชอบในการบริหารความเสี่ยง
15. Document Owner หมายถึง เจ้าของเอกสาร หรือ ผู้มีหน้าที่ความรับผิดชอบในการจัดทำ ทบทวน และปรับปรุง นโยบายการรักษาความมั่นคงปลอดภัยสารสนเทศ และเอกสารต่างๆ ที่เกี่ยวข้องในระบบ ISMS
16. All Personal หมายถึง พนักงานทุกคน รวมถึงบุคคลภายนอกที่เกี่ยวข้อง ผู้รับจ้าง ที่ปรึกษา พนักงานชั่วคราว คู่ค้า และผู้ให้บริการ ที่ใช้งานข้อมูลหรือระบบเทคโนโลยีสารสนเทศของคณะฯ

4. ขอบเขตระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ

โครงสร้างทางกายภาพพื้นฐาน และระบบสารสนเทศที่สนับสนุนศูนย์คอมพิวเตอร์แม่ข่ายหลักและศูนย์คอมพิวเตอร์แม่ข่ายสำรองของคณะแพทยศาสตร์ มหาวิทยาลัยเชียงใหม่

The Information Security Management System applies to physical security and supporting infrastructure of Data Center and Disaster Recovery Site of Faculty of Medicine, Chiang Mai University.

4.1 สถานที่

ศูนย์คอมพิวเตอร์แม่ข่ายหลัก (อาคารเรียนรวมราชนครินทร์ ชั้น M) และศูนย์คอมพิวเตอร์แม่ข่ายสำรอง (ศูนย์ความเป็นเลิศทางการแพทย์ อาคารเฉลิมพระเกียรติ 7 รอบพระชนมพรรษา ชั้น 7) คณะแพทยศาสตร์ มหาวิทยาลัยเชียงใหม่

เลขที่ 110 ถ.อินทวโรรส ต.ศรีภูมิ อ.เมือง จ.เชียงใหม่ 50200

4.2 หน่วยงานภายในคณะฯ ที่ให้การสนับสนุนระบบ ISMS โดยตรง

1. งานเทคโนโลยีสารสนเทศ
2. งานพัสดุและยานพาหนะ
3. งานบริหารงานบุคคล
4. งานซ่อมบำรุง

5. งานนโยบายและแผน
6. งานประชาสัมพันธ์
7. กองกฎหมาย

4.3 สิ่งที่ครอบคลุมในการขอรับรอง

ระบบการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศที่ขอรับรองมาตรฐานนี้ ได้มีการดำเนินการให้ครอบคลุมหัวข้อดังต่อไปนี้

1. เครื่องคอมพิวเตอร์ของผู้ดูแลระบบที่สนับสนุนการทำงานของศูนย์คอมพิวเตอร์แม่ข่ายหลักและศูนย์คอมพิวเตอร์แม่ข่ายสำรอง
2. บุคลากร พนักงาน และโครงสร้างการควบคุมของคณะฯ ที่เกี่ยวข้องกับการดำเนินงานตามขอบเขตที่กำหนด
3. โครงสร้างทางกายภาพพื้นฐานของศูนย์คอมพิวเตอร์แม่ข่ายหลักและศูนย์คอมพิวเตอร์แม่ข่ายสำรองของคณะฯ
4. ระบบสารสนเทศที่สนับสนุนการทำงานของศูนย์คอมพิวเตอร์แม่ข่ายหลักและศูนย์คอมพิวเตอร์แม่ข่ายสำรองของคณะฯ เช่น ระบบควบคุมการเข้าถึงทางกายภาพ ระบบกล้องวงจรปิด อุปกรณ์ตรวจจับควัน อุปกรณ์ตรวจจับน้ำรั่ว อุปกรณ์ดับเพลิง เครื่องปรับอากาศ อุปกรณ์กำเนิดไฟฟ้า อุปกรณ์สำรองไฟฟ้า เป็นต้น

4.4 ข้อยกเว้น

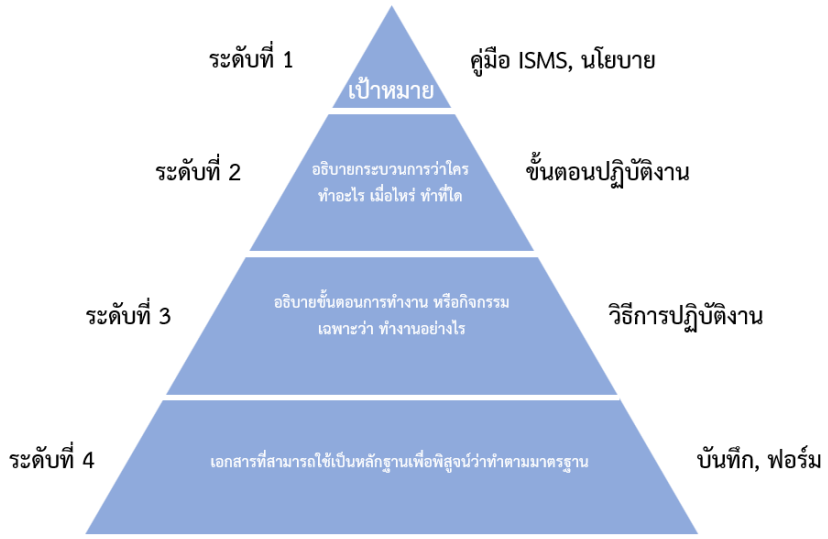
ระบบการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศที่ขอรับรองมาตรฐานนี้ ไม่ได้มีการดำเนินการให้ครอบคลุมหัวข้อดังต่อไปนี้

1. ระบบเทคโนโลยีสารสนเทศอื่นๆ นอกเหนือจากระบบที่สนับสนุนการทำงานของศูนย์คอมพิวเตอร์หลัก และศูนย์คอมพิวเตอร์สำรอง ที่ไม่อยู่ภายในขอบเขตการขอรับรองมาตรฐาน
2. หน่วยงานอื่นๆ และบุคลากรที่ไม่ได้ใช้งานระบบในขอบเขตการจัดทำ
3. คอมพิวเตอร์และอุปกรณ์ต่อพ่วงสำหรับผู้ใช้งานทั้งหมดของคณะฯ
4. การพัฒนาซอฟต์แวร์ที่ใช้เป็นเครื่องมือในการให้บริการ

5. เอกสารของระบบบริหารการจัดการความมั่นคงปลอดภัยสารสนเทศ

5.1 ประเภทเอกสาร

เอกสารระบบบริหารการจัดการความมั่นคงปลอดภัยสารสนเทศของคณะฯ แบ่งเป็น 4 ประเภทดังนี้



“ภาพประกอบประเภทเอกสารในระบบ ISMS”

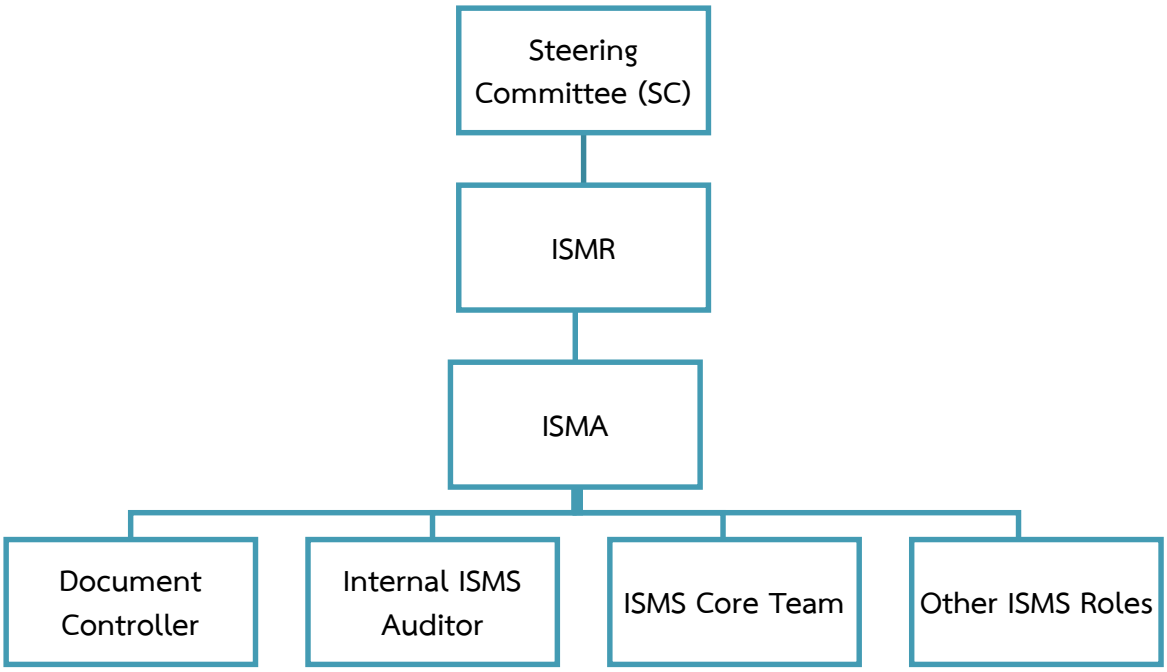
5.2 การควบคุมเอกสาร

1. เอกสารต้องได้รับการอนุมัติอย่างเหมาะสมก่อนประกาศใช้งาน
2. เอกสารต้องได้รับการทบทวนและปรับปรุงให้ทันสมัย และมีกระบวนการในการอนุมัติเอกสารใหม่ทุกครั้งที่มีการแก้ไขเปลี่ยนแปลงเอกสาร
3. การเปลี่ยนแปลงต่อเอกสาร และ เวอร์ชันล่าสุดของเอกสาร ต้องได้รับการเขียนระบุอย่างเหมาะสม
4. เอกสารเวอร์ชันล่าสุดต้องสามารถเข้าใช้งานได้โดยผู้ใช้งานที่เกี่ยวข้อง เมื่อมีความจำเป็นต้องใช้งาน
5. เอกสารต้องได้รับการป้องกันการเข้าถึงและใช้งานโดยผู้ที่ไม่เกี่ยวข้องหรือไม่มีสิทธิ์ในการใช้งาน
6. เอกสารต้องมีความครบถ้วนสมบูรณ์ และอยู่ในสภาพที่พร้อมใช้งาน
7. เอกสารต้องได้รับการจัดเก็บ ส่งผ่าน ใช้งาน และทำลาย ตามระดับความสำคัญของเอกสาร
8. เอกสารจากแหล่งภายนอก ที่มีการนำมาใช้งานในคณะฯ ต้องได้รับการขึ้นทะเบียนและควบคุมอย่างเหมาะสม
9. เอกสารเวอร์ชันเก่าที่ล้าสมัย ต้องได้รับการควบคุมและจัดเก็บ เพื่อป้องกันการนำไปใช้โดยมิได้ตั้งใจ และในกรณีที่จำเป็นต้องใช้งาน เอกสารต้องได้รับการเขียนระบุอย่างชัดเจน
10. อ้างอิง ขั้นตอนการปฏิบัติงานการควบคุมเอกสาร (Document Control Procedure)

5.3 การควบคุมบันทึก

บันทึกของระบบบริหารการจัดการความมั่นคงปลอดภัยสารสนเทศ ถือเป็นหลักฐานของการดำเนินงานตามระบบบริหารการจัดการความมั่นคงปลอดภัยสารสนเทศ ซึ่งต้องได้รับการปกป้องและควบคุมอย่างเหมาะสม เพื่อให้บันทึกอยู่ในสภาพที่ครบถ้วนสมบูรณ์ สามารถนำกลับมาตรวจสอบได้ และมีการปฏิบัติที่สอดคล้องตามกฎหมายหรือกฎระเบียบข้อบังคับที่เกี่ยวข้อง โดยการจัดเก็บ ใช้งาน และทำลายบันทึกต้องปฏิบัติตาม ขั้นปฏิบัติงานการควบคุมบันทึก (Record Control Procedure)

6. โครงสร้างและหน้าที่ความรับผิดชอบในระบบ ISMS



6.1 คณะกรรมการระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ

ISMS Steering Committee ประกอบด้วย ผู้บริหารระดับสูงจากส่วนงานที่เกี่ยวข้องที่ให้ความสนับสนุนในการจัดตั้ง ใช้งาน ตรวจสอบ และปรับปรุงระบบ ISMS ของคณะฯ ISMS Steering Committee มีหน้าที่ความรับผิดชอบดังนี้

1. กำหนดวัตถุประสงค์ด้านความมั่นคงปลอดภัยสารสนเทศของคณะฯ
2. อนุมัติและประกาศใช้งานนโยบายการรักษาความมั่นคงปลอดภัยสารสนเทศ และเอกสารต่างๆ ที่เกี่ยวข้องในระบบ ISMS
3. สื่อสารให้พนักงานทุกคนตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัยของข้อมูล และการปฏิบัติตามนโยบายการรักษาความมั่นคงปลอดภัยสารสนเทศ และเอกสารต่างๆ ในระบบ ISMS
4. ให้ความสนับสนุนในการให้ความรู้แก่พนักงานและบุคคลภายนอกที่เกี่ยวข้อง ให้รับทราบและสามารถปฏิบัติตามนโยบายการรักษาความมั่นคงปลอดภัยสารสนเทศ และเอกสารต่างๆ ที่

เกี่ยวข้องในระบบ ISMS รวมถึงตรวจสอบการปฏิบัติตามของพนักงานและบุคคลภายนอกที่เกี่ยวข้องอย่างเหมาะสม

5. พิจารณาลงโทษผู้ที่ละเมิดนโยบายการรักษาความมั่นคงปลอดภัยสารสนเทศ และเอกสารต่างๆ ที่เกี่ยวข้องในระบบ ISMS
6. กำหนดเกณฑ์ในการยอมรับความเสี่ยง และระดับความเสี่ยงที่ยอมรับได้ รวมถึงพิจารณาผลการประเมินความเสี่ยงและแผนการแก้ไขความเสี่ยงที่สำคัญของคณะฯ
7. ให้ความสนับสนุนด้านทรัพยากรที่จำเป็นในการจัดตั้ง ใช้งาน ตรวจสอบ และปรับปรุงระบบ ISMS
8. จัดประชุมเพื่อทบทวนการดำเนินงานของระบบ ISMS เพื่อให้มั่นใจว่าระบบ ISMS ของคณะฯ มีความเหมาะสม เพียงพอ และมีประสิทธิผล รวมถึงพิจารณาโอกาสในการปรับปรุงระบบ ISMS ให้ดีขึ้นอย่างต่อเนื่อง

6.2 ผู้บริหารระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ (ISMR) และผู้ช่วยผู้บริหารระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ (ISMA)

ISMR และ ISMA คือ ตัวแทนของผู้บริหารของคณะฯ ที่ทำหน้าที่ควบคุมดูแลการจัดตั้ง ใช้งาน ตรวจสอบ และปรับปรุงระบบ ISMS ของคณะฯ ISMR และ ISMA มีหน้าที่ความรับผิดชอบดังนี้

1. ประสานงานเพื่อจัดตั้งและพัฒนาระบบ ISMS ขึ้นในคณะฯ รวมถึงดูแลรักษา ตรวจสอบ และปรับปรุงระบบขึ้นอย่างต่อเนื่อง เพื่อให้บรรลุตามนโยบายการรักษาความมั่นคงปลอดภัยสารสนเทศ และสอดคล้องตามมาตรฐาน ISO 27001: 2013
2. ดูแลการปรับปรุงแก้ไขนโยบาย และเอกสารต่างๆ ที่เกี่ยวข้องในระบบ ISMS ให้เหมาะสมกับการเปลี่ยนแปลงที่เกิดขึ้น สอดคล้องกับมาตรฐาน ISO 27001: 2013 และคำแนะนำที่ได้รับจาก ISMS Steering Committee
3. สื่อสารให้พนักงานทุกคนรับทราบถึงหน้าที่และความรับผิดชอบของตนในการปฏิบัติตามนโยบายและเอกสารต่างๆ ที่เกี่ยวข้องของระบบ ISMS
4. สอดส่องดูแลการปฏิบัติงานของคณะฯ ให้เป็นไปตามที่กำหนดไว้ในเอกสารต่างๆ ของระบบ ISMS
5. ให้คำปรึกษาและแนะนำด้านการรักษาความมั่นคงปลอดภัยสารสนเทศและการนำนโยบายต่างๆ ไปใช้งาน แก่บุคลากรภายในคณะฯ
6. ให้มีการดำเนินกิจกรรมของระบบ ISMS ตามแผนที่วางไว้ และผลลัพธ์ที่ได้มีความสอดคล้องกับวัตถุประสงค์ด้านความมั่นคงปลอดภัยสารสนเทศของคณะฯ
7. ควบคุมดูแลการเปลี่ยนแปลง (Change) ต่างๆ ที่เกิดขึ้นในคณะฯ พร้อมทั้งประสานงานให้มีการประเมิน แก้ไขและควบคุมความเสี่ยงจากการเปลี่ยนแปลงอย่างเหมาะสม
8. ควบคุมดูแลการวัดประสิทธิผลของกระบวนการและมาตรการควบคุมต่างๆ (Controls) ในระบบ ISMS
9. ควบคุมดูแลการตรวจประเมินภายในของระบบ ISMS (Internal ISMS Audit) ให้เป็นไปอย่างเหมาะสม

10. ควบคุมดูแลการดำเนินการแก้ไขและป้องกันข้อบกพร่องในระบบ ISMS รวมถึงติดตามและทบทวนประสิทธิภาพของการแก้ไขและป้องกันอย่างเหมาะสม
11. ประสานงานเพื่อจัดให้มีการประชุมเพื่อทบทวนการดำเนินงานของระบบ ISMS โดยผู้บริหาร (Management Review) และติดตามการดำเนินการตามมติที่ประชุม
12. รายงานผลการดำเนินงานของระบบ ISMS ต่อผู้บริหาร
13. ประสานงานและหาแนวทางในการควบคุมและจัดการปัญหา ในกรณีที่เกิด Incident ขึ้นในคณะฯ

6.3 คณะทำงานระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ (ISMS CORE TEAM)

ISMS Core Team ประกอบด้วย ตัวแทนจากฝ่ายงานต่างๆ ที่อยู่ในขอบเขตของระบบ ISMS ที่ทำหน้าที่ในการประสานงานและดำเนินงานเกี่ยวกับระบบ ISMS ของแต่ละส่วนงาน ISMS Core Team มีหน้าที่ความรับผิดชอบดังนี้

1. สื่อสาร ให้คำแนะนำ และสอดส่องดูแลพนักงานในแต่ละส่วนงาน เพื่อให้สามารถปฏิบัติงานได้อย่างถูกต้องตามนโยบาย และเอกสารต่างๆ ที่เกี่ยวข้องในระบบ ISMS
2. จัดทำและปรับปรุงทะเบียนทรัพย์สินสารสนเทศในแต่ละส่วนงาน
3. ประสานงานกับ ISMR/ ISMA เพื่อทำการประเมินความเสี่ยงและบริหารจัดการความเสี่ยงสำหรับแต่ละฝ่ายงาน
4. ประสานงานกับ ISMR/ ISMA เพื่อดำเนินการตาม Security Plan ที่วางไว้
5. ประสานงานกับ ISMR/ ISMA เพื่อทำการวัดประสิทธิผลของกระบวนการและ Controls ในระบบ ISMS ที่เกี่ยวข้องในแต่ละส่วนงาน
6. จัดทำ “บัญชีรายชื่อบันทึก” (Record List) และดำเนินการควบคุมบันทึกสำหรับแต่ละส่วนงาน
7. ประสานงานกับ ISMR ในกรณีที่เกิดเหตุละเมิดความมั่นคง หรือเหตุฉุกเฉินใดๆ ขึ้นในคณะฯ เพื่อควบคุมและจัดการกับปัญหาที่เกิดขึ้น
8. รับฟังข้อร้องเรียนหรือข้อเสนอแนะที่เกี่ยวข้องกับระบบ ISMS จากพนักงานและบุคคลภายนอกที่เกี่ยวข้อง และดำเนินการตามที่ระบุในข้อ 12. การดำเนินการแก้ไข หรือรายงานต่อ ISMR เพื่อปรับปรุงการดำเนินงานของระบบ ISMS ให้มีประสิทธิภาพมากขึ้น

6.4 ผู้ควบคุมเอกสาร (Document Controller)

Document Controller คือ ผู้ทำหน้าที่ดูแลและควบคุมการใช้งานเอกสารและบันทึกต่างๆ ของระบบ ISMS ให้เป็นไปตามข้อกำหนดของมาตรฐาน ISO 27001: 2013 โดย Document Controller มีหน้าที่ความรับผิดชอบดังนี้

1. ควบคุมและดูแลกระบวนการสร้างเอกสารขึ้นใหม่ แก้ไขเปลี่ยนแปลงเอกสาร และยกเลิกเอกสาร
2. กำหนดเลขรหัสเอกสาร เวอร์ชันของเอกสาร และวันที่ของเอกสาร
3. จัดเก็บต้นฉบับของเอกสาร รวมถึงไฟล์ (Soft copy) ของเอกสาร
4. กำหนดสิทธิ์การเข้าถึงเอกสารให้แก่ผู้ที่เกี่ยวข้อง
5. เรียกคืนและควบคุมเอกสารที่ยกเลิกการใช้งาน

6. ควบคุมและดูแลให้มีการนำเอกสารไปใช้อย่างถูกต้องเหมาะสม รวมถึงควบคุมเมื่อมีการขอทำสำเนาเอกสาร หรือการนำเอกสารจากแหล่งภายนอกมาใช้งานในระบบ ISMS
7. จัดทำ Document Master List ของเอกสารระบบ ISMS ทั้งหมด และรับผิดชอบการปรับปรุงแก้ไขข้อมูลให้ถูกต้องอยู่เสมอ
8. ควบคุมและดูแลให้เอกสารได้รับการทบทวนและปรับปรุงให้ทันสมัย ตามรอบเวลาอย่างเหมาะสม

6.5 ผู้ตรวจสอบภายในระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ (INTERNAL ISMS AUDITOR)

Internal ISMS Auditor คือ ผู้ที่ได้รับมอบหมายให้ทำหน้าที่ตรวจประเมินภายในระบบ ISMS ของคณะฯ เพื่อหาความสอดคล้องและข้อบกพร่อง เพื่อนำไปสู่การปรับปรุงระบบ ISMS อย่างต่อเนื่อง Internal ISMS Auditor มีหน้าที่ความรับผิดชอบดังนี้

1. วางแผน ประสานงาน และดำเนินการตรวจประเมินภายในสำหรับระบบ ISMS ของคณะฯ
2. รายงานผลการตรวจประเมิน พร้อมทั้งให้คำแนะนำในการปรับปรุงแก่ผู้ที่เกี่ยวข้อง
3. ติดตามและตรวจสอบการดำเนินการแก้ไขหรือป้องกันข้อบกพร่องที่พบจากการตรวจประเมินภายใน

นอกจากนี้ได้มอบหมายให้ทำหน้าที่ติดตามตรวจสอบการปฏิบัติงานของพนักงานในแต่ละส่วนงาน ให้มีความสอดคล้องกับนโยบายการรักษาความมั่นคงปลอดภัยสารสนเทศ กระบวนการ ISMS และ Controls ที่เกี่ยวข้อง

1. ประสานงานกับ ISMS Core Team และส่วนงานที่เกี่ยวข้องในการกำหนดตัวชี้วัดประสิทธิผลของกระบวนการและ Controls ในระบบ ISMS ตลอดจนตัวชี้วัดความสอดคล้องในการปฏิบัติตามนโยบายการรักษาความมั่นคงปลอดภัยสารสนเทศ
2. ประสานงานกับ ISMS Core Team เพื่อทำการวัดประสิทธิผลของกระบวนการและ Controls ในระบบ ISMS และวัดความสอดคล้องในการปฏิบัติตามนโยบายการรักษาความมั่นคงปลอดภัยสารสนเทศ ที่เกี่ยวข้องในแต่ละส่วนงาน
3. วิเคราะห์ข้อมูลและรายงานผลการวัดประสิทธิผลและการวัดความสอดคล้อง ไปยัง ISMS Steering Committee, ISMR/ ISMA ตลอดจนผู้ที่เกี่ยวข้อง
4. ติดตามและตรวจสอบการดำเนินการแก้ไขหรือป้องกันข้อบกพร่องที่พบจากการวัดประสิทธิผลและการวัดความสอดคล้อง

6.6 เจ้าของสินทรัพย์

Asset Owner มีหน้าที่ความรับผิดชอบในการจัดทำทะเบียนทรัพย์สินสารสนเทศ กำหนดชั้นความลับสำหรับทรัพย์สินสารสนเทศประเภทข้อมูล และทำให้มั่นใจว่าทรัพย์สินสารสนเทศ จะได้รับการปกป้องอย่างเหมาะสม ตลอดระยะเวลาการใช้งานทรัพย์สินสารสนเทศ รวมถึงดูแลความมั่นคงปลอดภัยที่เกี่ยวข้องกับการทำลาย จำหน่ายออก โอนย้าย หรือยกเลิกการใช้งานทรัพย์สินสารสนเทศ

6.7 เจ้าของความเสี่ยง

Risk Owner มีหน้าที่ความรับผิดชอบในการประเมินความเสี่ยง วางแผนแก้ไขความเสี่ยง และทำให้มั่นใจว่าความเสี่ยงจะได้รับการแก้ไขตามแผน

6.8 เจ้าของเอกสาร

เจ้าของเอกสาร มีหน้าที่ความรับผิดชอบในการจัดทำ ทบทวน และปรับปรุง นโยบายการรักษาความมั่นคงปลอดภัยสารสนเทศ และเอกสารต่างๆ ที่เกี่ยวข้องในระบบ ISMS เพื่อให้มั่นใจว่าเอกสารมีความทันสมัยและสามารถนำไปใช้งานได้จริง Document Owner ต้องให้ความสนับสนุนในการประกาศใช้และปฏิบัติตามเอกสารเพื่อให้มั่นใจว่าบุคคลที่เกี่ยวข้องสามารถปฏิบัติงานตามเอกสารได้อย่างถูกต้อง

6.9 ผู้มีส่วนเกี่ยวข้องกับระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ

พนักงานทุกคน รวมถึงบุคคลภายนอกที่เกี่ยวข้อง ผู้รับจ้าง ที่ปรึกษา พนักงานชั่วคราว คู่ค้า และผู้ให้บริการ ที่ใช้งานข้อมูลหรือระบบเทคโนโลยีสารสนเทศของคณะฯ มีหน้าที่ความรับผิดชอบดังนี้

1. ปฏิบัติตามนโยบายการรักษาความมั่นคงปลอดภัยสารสนเทศ และเอกสารต่างๆ ที่เกี่ยวข้องของระบบ ISMS อย่างเคร่งครัด
2. ปกป้องและดูแลรักษาข้อมูลและทรัพย์สินสารสนเทศของคณะฯ อย่างเหมาะสม มิให้มีการเข้าถึง แก้ไข เปิดเผย หรือทำลายโดยบุคคลที่ไม่ได้รับอนุญาต
3. รับผิดชอบและปฏิบัติตามหน้าที่ที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยของข้อมูลและระบบเทคโนโลยีสารสนเทศที่ได้รับมอบหมายอย่างเหมาะสม
4. รายงานสิ่งผิดปกติหรือจุดอ่อนด้านความมั่นคงที่พบเห็นต่อคณะฯ อย่างเหมาะสม

7. การกำหนดวัตถุประสงค์และวางแผนการรักษาความมั่นคงปลอดภัยสารสนเทศ

7.1 การกำหนดวัตถุประสงค์ด้านความมั่นคงปลอดภัยสารสนเทศของคณะฯ

การกำหนดวัตถุประสงค์ด้านความมั่นคงปลอดภัยสารสนเทศในระดับฝ่ายงานที่มีความสอดคล้องกับวัตถุประสงค์ทางการดำเนินงาน วัตถุประสงค์ที่กำหนดไว้ในนโยบายการรักษาความมั่นคงปลอดภัยสารสนเทศ และวัตถุประสงค์ของระบบ ISMS เพื่อกำหนดทิศทางในการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศภายในคณะฯ ให้สอดคล้องกับวัตถุประสงค์ทางการดำเนินงาน ความต้องการและความคาดหวังของผู้ที่เกี่ยวข้อง

7.2 การวางแผนการรักษาความมั่นคงปลอดภัยสารสนเทศ

จัดทำแผนการรักษาความมั่นคงปลอดภัยสารสนเทศของคณะฯ เพื่อกำหนดกิจกรรมที่ต้องดำเนินการเพื่อให้บรรลุวัตถุประสงค์ด้านการรักษาความมั่นคงปลอดภัยสารสนเทศของคณะฯ ที่ได้กำหนดไว้ กำหนดการ และผู้รับผิดชอบ

8. ระบบบริหารความมั่นคงปลอดภัยสารสนเทศ (Information Security Management System)

ระบบบริหารความมั่นคงปลอดภัยสารสนเทศ หรือ ระบบ ISMS ของคณะฯได้รับการจัดตั้ง ใช้งาน ตรวจสอบ และปรับปรุงอย่างต่อเนื่อง ตามข้อกำหนดของมาตรฐาน ISO 27001:2013 โดยใช้หลักการบริหารความเสี่ยง เพื่อสร้างความมั่นใจให้กับผู้ที่เกี่ยวข้อง ว่าข้อมูลและระบบสารสนเทศที่

สำคัญของคณะฯ จะได้รับปกป้องอย่างเหมาะสม นอกจากนี้ระบบ ISMS ยังได้รับการออกแบบให้สามารถทำงานได้อย่างสอดคล้องกับกระบวนการและโครงสร้างการบริหารงานของคณะฯ โดยครอบคลุมกิจกรรมที่สำคัญดังต่อไปนี้

1. การกำหนดความต้องการของคณะฯ ในการรักษาความมั่นคงปลอดภัยสารสนเทศ และการประกาศใช้งานนโยบายการรักษาความมั่นคงปลอดภัยสารสนเทศ รวมถึงการสื่อสารให้ผู้ที่เกี่ยวข้องรับทราบ
2. การประเมินความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศของคณะฯ
3. การสร้างมาตรการควบคุมที่สอดคล้องกับความเสี่ยงของคณะฯ
4. การตรวจสอบและวัดผลการดำเนินงานและประสิทธิผลของระบบ ISMS
5. การปรับปรุงอย่างต่อเนื่องที่สอดคล้องตามผลการวัดและวัตถุประสงค์ที่วางไว้

องค์ประกอบหลักของระบบระบบบริหารความมั่นคงปลอดภัยสารสนเทศ ของคณะฯ แสดงได้ดังแผนภาพ ดังนี้

ภาพแสดงองค์ประกอบหลักของระบบระบบบริหารความมั่นคงปลอดภัยสารสนเทศ

8.1 Clause 4 การวิเคราะห์บริบทที่เกี่ยวข้องและการกำหนดขอบเขตของระบบ ISMS (Context of the organization)

ทำการวิเคราะห์บริบทภายในและภายนอก รวมถึงความคาดหวังของผู้ที่เกี่ยวข้อง เพื่อกำหนดวัตถุประสงค์ด้านการรักษาความมั่นคงปลอดภัยสารสนเทศของคณะฯ และขอบเขตของระบบ ISMS

8.2 Clause 5 การชี้นำคณะฯ โดยผู้บริหาร (Leadership)

ผู้บริหารให้ความสำคัญและให้ความสนับสนุนการดำเนินงานของระบบ ISMS โดยการประกาศนโยบายการรักษาความมั่นคงปลอดภัยข้อมูลสารสนเทศ กำหนดหน้าที่ความรับผิดชอบของพนักงาน ทบทวนการดำเนินงานของระบบ ISMS และจัดสรรทรัพยากรที่จำเป็นในการดำเนินงานและปรับปรุงระบบ ISMS อย่างต่อเนื่อง อ้างอิง Information Security Policy

8.3 Clause 6 การวางแผนการดำเนินงานของระบบ ISMS (Planning)

ทำการวางแผนการรักษาความมั่นคงปลอดภัยข้อมูลสารสนเทศของคณะฯ เพื่อกำหนดกิจกรรมที่ต้องดำเนินการเพื่อให้บรรลุวัตถุประสงค์ด้านการรักษาความมั่นคงปลอดภัยข้อมูลสารสนเทศของคณะฯ ที่ได้กำหนดไว้ ตลอดจนทำการวิเคราะห์ความเสี่ยงด้านความมั่นคงปลอดภัยข้อมูลสารสนเทศ รวมถึงความเสี่ยงที่อาจส่งผลต่อการดำเนินงานของระบบ ISMS และวางแผนแก้ไขความเสี่ยงโดยเลือกใช้งานมาตรการควบคุมที่สมเหตุสมผล

8.4 Clause 7 การสนับสนุนการดำเนินงานของระบบ ISMS (Support)

ทำการบริหารทรัพยากรที่จำเป็นต่อการดำเนินงานของระบบ ISMS โดยเฉพาะอย่างยิ่งทรัพยากรบุคคลให้มีความรู้ความสามารถ และความตระหนักถึงความจำเป็นในการปฏิบัติตามนโยบายการรักษาความมั่นคงปลอดภัยข้อมูลสารสนเทศและกระบวนการของระบบ ISMS

8.5 Clause 8 การดำเนินงานของระบบ ISMS (Operation)

กำกับดูแลการดำเนินงานของระบบ ISMS และกิจกรรมการแก้ไขความเสี่ยงให้มีประสิทธิผลและเป็นไปตามแผนที่วางไว้ รวมถึงติดตามให้มีการประเมินความเสี่ยงและวางแผนแก้ไขความเสี่ยงอย่างสม่ำเสมอ หรือเมื่อมีความเปลี่ยนแปลงที่สำคัญที่อาจส่งผลต่อความเสี่ยงของคณะฯ

8.6 Clause 9 การประเมินประสิทธิผลของระบบ ISMS (Performance Evaluation)

ทำการตรวจสอบและประเมินประสิทธิผลของกระบวนการและมาตรการควบคุมต่างๆ เปรียบเทียบกับนโยบายการรักษาความมั่นคงปลอดภัยข้อมูลสารสนเทศ มาตรฐานที่เกี่ยวข้อง ตัวชี้วัด และวัตถุประสงค์ด้านการรักษาความมั่นคงปลอดภัยข้อมูลสารสนเทศของคณะฯ และรายงานผลต่อผู้บริหาร

8.7 Clause 10 การปรับปรุงระบบ ISMS อย่างต่อเนื่อง (Improvement)

ทำการแก้ไขข้อบกพร่องที่พบจากการตรวจสอบและประเมินประสิทธิผลของกระบวนการและมาตรการควบคุมต่างๆ รวมถึงทำการปรับปรุงระบบ ISMS อย่างต่อเนื่อง โดยการทบทวนและปรับปรุงวัตถุประสงค์ด้านการรักษาความมั่นคงปลอดภัยข้อมูลสารสนเทศของคณะฯ และแผนงานที่เกี่ยวข้อง

9. การสนับสนุนการดำเนินงานของระบบ ISMS

9.1 การจัดฝึกอบรม การให้ความรู้ และความสามารถของพนักงาน

ISMR/ISMA และหัวหน้างาน ต้องให้ความสนับสนุนในการจัดฝึกอบรม ให้ความรู้แก่พนักงานที่เกี่ยวข้องที่ได้รับมอบหมายหน้าที่ความรับผิดชอบในระบบ ISMS อย่างเหมาะสมและเพียงพอต่อการปฏิบัติงาน โดย

1. ระบุความสามารถที่จำเป็นสำหรับพนักงานที่ทำหน้าที่เกี่ยวข้องกับระบบ ISMS
2. จัดให้มีการฝึกอบรม หรือจัดหาบุคลากรที่มีความรู้เข้าทำงาน (ในกรณีที่จำเป็น)
3. ประเมินประสิทธิผลของการฝึกอบรม และดำเนินการตามความเหมาะสม

4. จัดเก็บบันทึกของการฝึกอบรม ตลอดจนหลักฐานอื่นๆ ที่เป็นเครื่องยืนยันความรู้ความสามารถและประสบการณ์ของพนักงาน

ISMR/ISMA และหัวหน้างานต้องทำให้พนักงานที่มีหน้าที่เกี่ยวข้องกับระบบ ISMS ตระหนักถึงความสำคัญของหน้าที่ความรับผิดชอบของตนในการรักษาความมั่นคงปลอดภัยของข้อมูล และช่วยให้คณะฯ ประสบความสำเร็จตามวัตถุประสงค์ที่กำหนดไว้

9.2 การสื่อสารภายในและภายนอก

จัดทำแผนการสื่อสาร (Security Communication Plan) เพื่อสื่อสารข้อมูลที่จำเป็นต่อการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศไปยังผู้ที่เกี่ยวข้องทั้งภายในและภายนอกคณะฯ

1. การสื่อสารภายในคณะฯ หมายถึง การสื่อสารระหว่างส่วนงาน และการรายงานต่อผู้บริหาร
2. การสื่อสารภายนอกคณะฯ หมายถึง การสื่อสารระหว่างคณะฯ กับหน่วยงานภายนอก เช่น คู่ค้า ผู้ให้บริการภายนอก หรือหน่วยงานภาครัฐที่เกี่ยวข้อง และการสื่อสารระหว่างคณะฯ กับบุคคลภายนอก เช่น ผู้รับบริการ บุคคลทั่วไป เป็นต้นอ้างอิง Security Communication Plan

9.3 การกำกับดูแลการปฏิบัติงานของผู้ให้บริการภายนอก

ทำการกำกับดูแลผู้ให้บริการภายนอกที่ดำเนินกิจกรรมหรือกระบวนการด้านการรักษาความมั่นคงปลอดภัยข้อมูลสารสนเทศให้แก่คณะฯ โดยควบคุมให้กิจกรรมหรือกระบวนการดังกล่าว เป็นไปตามนโยบายด้านการรักษาความมั่นคงปลอดภัยข้อมูลสารสนเทศของคณะฯ ตลอดจนเอกสารสนับสนุนอื่นๆ ที่เกี่ยวข้อง พร้อมทั้งทำการประเมินผลผู้ให้บริการภายนอกและสนับสนุนให้มีการปรับปรุงอย่างต่อเนื่อง

10. การบริหารจัดการความเสี่ยง

การบริหารจัดการความเสี่ยง คือกระบวนการที่เป็นระบบ ในการระบุความเสี่ยง ประเมินความเสี่ยง และแก้ไขควบคุมความเสี่ยงให้อยู่ในระดับที่คณะฯ สามารถยอมรับได้ กระบวนการบริหารจัดการความเสี่ยงถือเป็นหัวใจสำคัญที่ทำให้ระบบ ISMS ของคณะฯ สามารถรักษาไว้ซึ่งความมั่นคงปลอดภัยสารสนเทศ โดยการบริหารจัดการความเสี่ยงเป็นงานที่ต้องดำเนินการอย่างต่อเนื่องเพื่อแก้ไขและควบคุมความเสี่ยงที่อาจเกิดขึ้นจากการเปลี่ยนแปลงทั้งจากภายในและภายนอกคณะฯ

มาตรฐานที่ใช้อ้างอิงในการบริหารจัดการความเสี่ยงของคณะฯ

1. ISO 31000:2009, Risk Management – Principles and guidelines
2. ISO/IEC 27005:2011, Information technology - Security techniques - Information security risk management

10.1 เกณฑ์ในการยอมรับความเสี่ยงและระดับความเสี่ยงที่สามารถยอมรับได้

คณะฯ จัดแบ่งระดับความเสี่ยงเป็น 5 ระดับ คือ Extreme, High, Medium, Low และ Very Low โดยระดับความเสี่ยงที่คณะฯ สามารถยอมรับได้โดยไม่จำเป็นต้องดำเนินการแก้ไขและควบคุมความเสี่ยงคือ ระดับ Very Low และ Low เท่านั้น การยอมรับความเสี่ยงที่เกินกว่า Low ต้องดำเนินการอย่างเป็นลายลักษณ์อักษรและต้องได้รับความเห็นชอบจากผู้บริหารที่เกี่ยวข้อง โดยหลักเกณฑ์ในการยอมรับความเสี่ยงที่เป็นไปได้คือ

1. การลงทุนเพื่อแก้ไขและควบคุมความเสี่ยงไม่คุ้มค่าเมื่อเทียบกับผลกระทบสูงสุดที่สามารถเกิดขึ้นได้
2. ความเสี่ยงไม่สามารถแก้ไขและควบคุมให้ลดลงมาอยู่ในระดับ Very Low หรือ Low ได้
3. การตัดสินใจของผู้บริหารที่จะไม่ดำเนินการกับความเสี่ยงนั้น ซึ่งต้องมีเหตุผลสนับสนุนที่เหมาะสม

10.2 กระบวนการบริหารจัดการความเสี่ยง

กิจกรรมหลักของกระบวนการบริหารจัดการความเสี่ยงมี 3 ส่วนคือ

1. การประเมินความเสี่ยง (Risk Assessment)
   การประเมินความเสี่ยง คือ การวิเคราะห์หาค่าความเสี่ยงโดยพิจารณาถึงเหตุการณ์ความเสี่ยง (Risk Scenario) ที่เป็นไปได้ โดยเหตุการณ์ความเสี่ยงนี้มีนัยครอบคลุมภัยคุกคาม (Threat) และจุดอ่อน (Vulnerability) ที่เกี่ยวข้อง จากนั้นจึงดำเนินการประเมินค่าความเป็นไปได้ (Likelihood) ที่จะเกิดความเหตุการณ์ความเสี่ยงขึ้น และประเมินค่าผลกระทบ (Consequence) จากเหตุการณ์ความเสี่ยงนั้น โดย อ้างอิงตาม ขั้นตอนการปฏิบัติงาน การบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ (Risk Management Procedure)

2. การแก้ไขและควบคุมความเสี่ยง (Risk Treatment)
   การแก้ไขและควบคุมความเสี่ยง คือ การหาวิธีการหรือเครื่องมือต่างๆ ที่เหมาะสม เพื่อแก้ไขและควบคุมความเสี่ยงให้อยู่ในระดับที่คณะฯ สามารถยอมรับได้ โดยมีแนวทางที่เป็นไปได้ในการแก้ไขและควบคุมความเสี่ยง ดังนี้
   1. แก้ไขความเสี่ยง
   2. ยอมรับความเสี่ยง
   3. หลีกเลี่ยงความเสี่ยง
   4. โอนหรือแบ่งปันความเสี่ยงกับหน่วยงานอื่น
   5. ยอมให้ความเสี่ยงเพิ่มขึ้น เพื่อโอกาสทางการดำเนินงาน

   การเลือกแนวทางเพื่อแก้ไขและควบคุมความเสี่ยงต้องพิจารณาความเหมาะสมและทรัพยากรที่ต้องใช้ ทั้งนี้ การดำเนินการแก้ไขความเสี่ยง ให้อ้างอิงวิธีการแก้ไขจากมาตรการควบคุมต่างๆ (Controls) ใน Annex A ของมาตรฐาน ISO 27001: 2013
3. การทบทวนการประเมินความเสี่ยง (Review of Risk Assessment)
   ผลการประเมินความเสี่ยงต้องได้รับการทบทวนตามรอบเวลาที่กำหนดไว้อย่างเหมาะสม อย่างน้อยปีละ 1 ครั้ง หรือเมื่อมีการเปลี่ยนแปลงที่สำคัญเกิดขึ้น เพื่อให้มั่นใจว่าวิธีการที่ใช้และผลการประเมินความเสี่ยงสอดคล้องกับสถานการณ์ปัจจุบัน และไม่มีข้อผิดพลาด

11. การประเมินประสิทธิผล (Performance Evaluation)

การประเมินประสิทธิผล เป็นกระบวนการสำคัญที่แสดงให้เห็นถึงประสิทธิผล และการพัฒนาอย่างต่อเนื่องของระบบ ISMS ซึ่งช่วยให้คณะฯ ทราบว่า นโยบาย เอกสารสนับสนุน กระบวนการ มาตรการควบคุม และแนวทางการแก้ไขและควบคุมความเสี่ยงต่างๆ ที่เลือกใช้มีประสิทธิผลดีเพียงใด โดยทำการ

ประเมินประสิทธิผลทั้งในส่วนของ ISMS Requirements (Clause 4 – 10) และ มาตรการควบคุมต่างๆ (Controls) ที่เลือกใช้งานใน Annex A ของมาตรฐาน ISO 27001: 2013

ตัวชี้วัดที่ใช้ในการประเมินประสิทธิผล มีทั้งตัวชี้วัดก่อนเกินเหตุ (Lead Indicator) และตัวชี้วัดหลังเกิดเหตุ (Lag Indicator) เพื่อให้ได้รับข้อมูลที่ครอบคลุม ผลที่ได้จากการประเมินประสิทธิผลจะถูกรายงานไปยังผู้บริหารและผู้ที่เกี่ยวข้อง เพื่อพิจารณาดำเนินการแก้ไขหรือปรับปรุงระบบ ISMS ต่อไป อ้างอิง ขั้นตอนการปฏิบัติงานการวัดและควบคุมประสิทธิผล (Effectiveness Measurement Procedure)

12. การตรวจประเมินภายในของระบบ ISMS

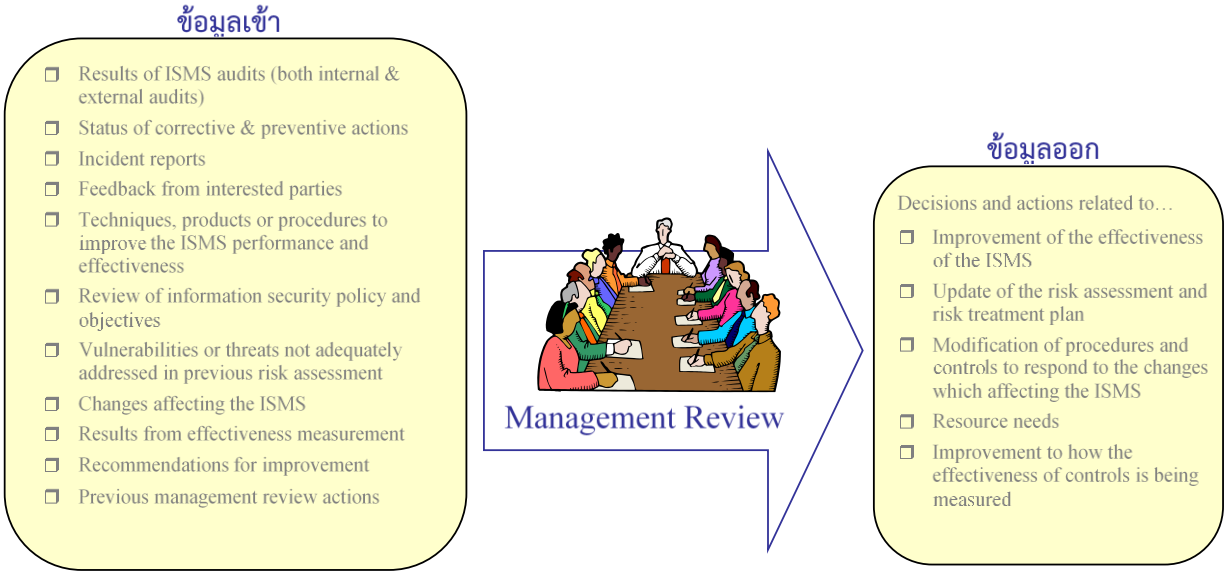
คณะฯ จัดให้มีการตรวจประเมินภายในสำหรับระบบ ISMS อย่างน้อยปีละ 1 ครั้ง เพื่อให้มั่นใจว่าการดำเนินงานของระบบ ISMS

1. เป็นไปตามข้อกำหนดของมาตรฐาน ISO 27001:2013 และ กฎหมายกฎระเบียบต่างๆ ที่เกี่ยวข้อง
2. เป็นไปตามข้อกำหนดและเอกสารของระบบ ISMS ของคณะฯ
3. มีการนำไปปฏิบัติอย่างมีประสิทธิผล

การวางแผนการตรวจประเมินภายในต้องพิจารณาถึงความสำคัญของกระบวนการ ส่วนงาน หรือพื้นที่ที่จะทำการตรวจประเมิน และผลจากการตรวจประเมินในครั้งก่อน โดยผู้ทำการตรวจประเมินต้องได้รับการฝึกอบรม และคัดเลือกอย่างเหมาะสม มิให้มีการตรวจประเมินงานในส่วนที่ตนมีส่วนเกี่ยวข้อง ทั้งนี้ การวางแผน การดำเนินการตรวจประเมิน การรายงานผล และการติดตามทบทวนการแก้ไข ให้ปฏิบัติตาม Internal ISMS Audit Procedure โดยผู้บริหารของส่วนงานที่ถูกตรวจประเมินต้องให้ความร่วมมือในการหาสาเหตุและดำเนินการแก้ไขข้อบกพร่องที่ตรวจพบ

13. การทบทวนระบบ ISMS โดยผู้บริหาร

ISMS Steering Committee ต้องจัดประชุมเพื่อทบทวนการดำเนินงานของระบบ ISMS อย่างน้อยปีละ 1 ครั้ง เพื่อให้มั่นใจว่าการดำเนินงานของระบบ ISMS ของคณะฯ มีความเหมาะสม เพียงพอ และมีประสิทธิผล การทบทวนดังกล่าวต้องพิจารณาถึงโอกาสในการปรับปรุงระบบ ISMS และการเปลี่ยนแปลงต่างๆ ที่จำเป็นต้องดำเนินการ รวมถึงพิจารณาทบทวนและปรับปรุงนโยบายการรักษาความมั่นคงปลอดภัยสารสนเทศ และวัตถุประสงค์ในการรักษาความมั่นคงปลอดภัยสารสนเทศของคณะฯ ทั้งนี้ ผลการทบทวนต้องได้รับการบันทึกไว้อย่างเหมาะสม



ภาพแสดงประกอบการทบทวนระบบระบบบริหารความมั่นคงปลอดภัยสารสนเทศโดยผู้บริหาร

14. การดำเนินการแก้ไข

คณะฯ จัดให้มีกระบวนการดำเนินการแก้ไข (Corrective Action) เพื่อกำจัดสาเหตุของปัญหาหรือข้อบกพร่อง (Nonconformity) ที่พบในระบบ ISMS เพื่อป้องกันมิให้เกิดซ้ำ โดยการดำเนินการทั้งหมดต้องได้รับการสื่อสารไปยังพนักงานที่เกี่ยวข้องตามความเหมาะสม และมีการติดตามและตรวจสอบผลการดำเนินการเพื่อให้มั่นใจว่าบรรลุตามวัตถุประสงค์ของการดำเนินการ อ้างอิง Corrective Action Procedure

15. Statement of Applicability (SoA)

Statement of Applicability หรือ SoA คือ เอกสารที่ระบุถึงการประยุกต์ใช้มาตรการควบคุมต่างๆ (Controls) ทั้ง 114 ข้อของมาตรฐาน ISO 27001: 2013 ของคณะฯ โดยระบุถึง

1. มาตรการควบคุมต่างๆ (Controls) ที่ได้เลือกใช้งานในระบบ ISMS พร้อมด้วยคำอธิบายของการประยุกต์ใช้งาน หรือ อ้างอิงถึงเอกสารที่เกี่ยวข้องที่สามารถอธิบายการประยุกต์ใช้มาตรการต่างๆ (Controls) นั้นๆ ได้
2. มาตรการควบคุมต่างๆ (Controls) ที่มิได้นำมาประยุกต์ใช้งาน พร้อมเหตุผลของการไม่นำมาใช้ อ้างอิง Statement of Applicability

16. การปรับปรุงระบบ ISMS อย่างต่อเนื่อง

คณะฯ ให้ความสำคัญต่อการปรับปรุงระบบ ISMS อย่างต่อเนื่อง เพื่อให้การรักษาความมั่นคงปลอดภัยข้อมูลสารสนเทศมีประสิทธิผล และสามารถปกป้องทรัพย์สินสารสนเทศ ข้อมูล และระบบสารสนเทศที่สำคัญของคณะฯ จากภัยคุกคามที่มีการเปลี่ยนแปลงหรือเกิดขึ้นใหม่อยู่เสมอ โดยทำการทบทวนบริบทภายในและภายนอก ตลอดจนความต้องการและความคาดหวังของผู้ที่เกี่ยวข้อง เพื่อปรับปรุงวัตถุประสงค์ในการรักษาความมั่นคงปลอดภัยข้อมูลสารสนเทศและแผนการรักษาความมั่นคงปลอดภัยข้อมูลสารสนเทศของคณะฯ เป็นประจำทุกปี