นโยบายด้านความมั่นคงปลอดภัยสารสนเทศ
Information Security Policy

คณะแพทยศาสตร์ มหาวิทยาลัยเชียงใหม่

รหัสเอกสาร : ISMS-PL-I-002
ฉบับที่ : 2.0
ประเภทเอกสาร : เอกสารภายใน

สารบัญ

การควบคุมเอกสาร

การอนุมัติใช้เอกสาร

เอกสารนี้ผ่านการทบทวนและอนุมัติโดย:

จัดเตรียมเอกสารโดย	ทบทวนเอกสารโดย	อนุมัติเอกสารโดย
(นางสาวอลิศา นิ่มวรพันธุ์) คณะทำงานระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ	(นางอัจฉราภรณ์ อังศุรัตนเวช) ผู้บริหารระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ	(ศาสตราจารย์ (เชี่ยวชาญพิเศษ) นายแพทย์บรรณกิจ โลจนาภิวัฒน์) ประธานกรรมการอำนวยการระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ
วันที่ 26 มกราคม 2566	วันที่ 1 กุมภาพันธ์ 2566	วันที่ 7 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

นโยบายด้านความมั่นคงปลอดภัยสารสนเทศ (Information Security Policy)

1. วัตถุประสงค์

เพื่อปกป้องข้อมูลและระบบสารสนเทศของคณะแพทยศาสตร์ มหาวิทยาลัยเชียงใหม่ (คณะฯ) โดยเฉพาะทรัพย์สินที่สำคัญ ภายใต้ขอบเขตของระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ (ISMS) ให้มีความมั่นคงปลอดภัย และเพิ่มความเชื่อมั่นแก่ผู้ที่เกี่ยวข้อง โดยปกป้องไม่ให้ระบบสารสนเทศสามารถเข้าถึงได้โดยไม่ได้รับอนุญาต ปกป้องจากภัยคุกคามและความเสี่ยงที่มี ทั้งจากภายใน และภายนอกคณะฯ

2. ขอบเขต

ขอบเขตของนโยบายด้านความมั่นคงปลอดภัยสารสนเทศ ครอบคลุมการดำเนินงานของบุคคล/หน่วยงานที่อยู่ภายใต้ขอบเขตการขอรับรองมาตรฐาน รวมถึงข้อมูล ทรัพย์สิน และบุคลากรที่เกี่ยวข้อง

3. คำจำกัดความ

-

4. นโยบาย

1. จัดให้มีนโยบายด้านความมั่นคงปลอดภัยสารสนเทศ และนโยบายที่เกี่ยวข้องกับการดำเนินการในระบบสารสนเทศที่เป็นลายลักษณ์อักษร ซึ่งได้รับการอนุมัติจากผู้บริหารระดับสูง รวมถึงการแก้ไขเปลี่ยนแปลงต้องได้รับการอนุมัติก่อนเผยแพร่ทุกครั้ง
2. นโยบายที่จัดทำต้องมีการกำหนดวัตถุประสงค์ ขอบเขต ความรับผิดชอบ และเนื้อหาอย่างชัดเจน
3. นโยบายที่จัดทำต้องมีการเผยแพร่ให้บุคคลที่เกี่ยวข้องรับทราบ และปฏิบัติตาม รวมถึงมีการจัดเก็บให้ผู้ที่ใช้งาน และผู้ที่เกี่ยวข้องเข้าถึงได้ง่าย
4. มีการทบทวนและปรับปรุงนโยบายอย่างน้อยปีละ 1 ครั้ง ให้สอดคล้องต่อความต้องการของคณะฯ ในด้านของการรักษาความมั่นคงปลอดภัยสารสนเทศ เพื่อรับมือต่อภัยคุกคามในรูปแบบต่างๆที่อาจจะส่งผลต่อการดำเนินงานของทางคณะฯ ทั้งในปัจจุบัน และในอนาคต
5. ข้อมูลที่สำคัญของคณะฯ ต้องได้รับการรักษาความลับอย่างเหมาะสม มีความถูกต้องและสมบูรณ์ครบถ้วน รวมถึงต้องมีความพร้อมใช้งานอยู่เสมอ
6. บุคลากรในขอบเขต ต้องได้รับการฝึกอบรมด้านความมั่นคงปลอดภัยสารสนเทศ
7. มีการกำหนดระดับความเสี่ยงที่ยอมรับได้ในระบบสารสนเทศ และกำหนดมาตรการหรือวิธีปฏิบัติในการควบคุมความเสี่ยง
8. จัดให้มีการบริหารจัดการความเสี่ยง (Risk Management) ที่เกี่ยวข้องกับความมั่นคงปลอดภัยสารสนเทศของคณะฯ
9. จัดให้มีการประเมินความเสี่ยงในระบบสารสนเทศอย่างน้อยปีละ 1 ครั้ง หรือ เมื่อมีการเปลี่ยนแปลงที่สำคัญในระบบสารสนเทศ ซึ่งต้องมีการรายงานผลการประเมินความเสี่ยงแก่ผู้บริหารระดับสูงให้รับทราบ
10. จัดให้มีกระบวนการในการรายงาน สืบสวน รับมือ และจัดการกับเหตุการณ์ละเมิดความมั่นคงปลอดภัยสารสนเทศอย่างเหมาะสม
11. กำหนดกระบวนการในการดำเนินงานอย่างต่อเนื่อง เมื่อเกิดสภาวะฉุกเฉินหรือภัยพิบัติ โดยต้องคำนึงถึงความสำคัญด้านการดำเนินการอย่างต่อเนื่อง และการรักษาความมั่นคงปลอดภัยที่ดี โดยดำเนินการจัดทำแผน ดูแลรักษา และทดสอบแผนอย่างเหมาะสม
12. มีการตรวจสอบ รวมถึงประเมินการดำเนินการตามนโยบายอย่างน้อยปีละ 1 ครั้งเพื่อประเมินประสิทธิภาพ ประสิทธิผล และความเพียงพอของนโยบาย

5. บทลงโทษ

การละเมิด ฝ่าฝืน หรือไม่ปฏิบัติตามนโยบาย รวมวิธีปฏิบัติงาน และเอกสารที่เกี่ยวข้อง ไม่ว่าโดยเจตนา หรือไม่เจตนา ถือเป็นความผิดซึ่งต้องถูกลงโทษทางวินัยตามความเหมาะสม หากการละเมิด ฝ่าฝืน หรือไม่ปฏิบัติตามเข้าข่ายการกระทำความผิดทางกฎหมาย ผู้ละเมิดต้องได้รับการดำเนินคดีทางกฎหมาย ตามที่กฎหมายระบุไว้