นโยบายโต๊ะทำงานปลอดเอกสารสำคัญ และนโยบายการป้องกันหน้าจอคอมพิวเตอร์ Clear desk Clear screen Policy

คณะแพทยศาสตร์ มหาวิทยาลัยเชียงใหม่

รหัสเอกสาร : ISMS-PL-I-012
ฉบับที่ : 2.0
ประเภทเอกสาร : เอกสารภายใน

สารบัญ

การควบคุมเอกสาร.....1

นโยบายโต๊ะทำงานปลอดเอกสารสำคัญและนโยบายการป้องกันหน้าจอคอมพิวเตอร์ CLEAR DESK CLEAR SCREEN POLICY 2

1. วัตถุประสงค์.....2

2. ขอบเขต 2

3. นโยบาย.....2

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

นโยบายโต๊ะทำงานปลอดเอกสารสำคัญและนโยบายการป้องกันหน้าจอคอมพิวเตอร์

Clear desk Clear screen Policy

1. วัตถุประสงค์

เพื่อปกป้องข้อมูลและระบบสารสนเทศของคณะแพทยศาสตร์ มหาวิทยาลัยเชียงใหม่ (คณะฯ) โดยเฉพาะทรัพย์สินที่สำคัญ ภายใต้ขอบเขตของระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ (ISMS) ให้มีความมั่นคงปลอดภัย และเพิ่มความเชื่อมั่นแก่ผู้ที่เกี่ยวข้อง ต้องควบคุมไม่ให้สินทรัพย์สารสนเทศ เช่น เอกสาร สื่อบันทึกข้อมูลคอมพิวเตอร์ หรือสารสนเทศ อยู่ในภาวะซึ่งเสี่ยงต่อการเข้าถึงโดยผู้ซึ่งไม่มีสิทธิ์ และต้องกำหนดให้ผู้ใช้งานออกจากระบบสารสนเทศเมื่อว่างเว้นจากการใช้งาน

2. ขอบเขต

ขอบเขตของนโยบายด้านความมั่นคงปลอดภัยสารสนเทศ ครอบคลุมการดำเนินงานของบุคคล/หน่วยงานที่อยู่ภายใต้ขอบเขตการขอรับรองมาตรฐาน รวมถึงข้อมูล ทรัพย์สิน และบุคลากร ที่เกี่ยวข้อง

3. นโยบาย

ผู้ใช้ทุกคนควรจะตระหนักถึงความต้องการความปลอดภัยและวิธีการสำหรับการปกป้องอุปกรณ์ในขณะที่ผู้ใช้งานไม่อยู่ และมีความรับผิดชอบในการดำเนินการป้องกันดังกล่าว ดังนี้

1) ปิดการใช้งาน Active Session เมื่อทำงานเสร็จ หรือหากยังจำเป็นต้องเปิดไว้ เพราะยังทำงานค้างอยู่ ก็ต้องมีการรักษาความปลอดภัยโดยกลไกการล็อคที่เหมาะสม เช่น โปรแกรมรักษาหน้าจอป้องกันด้วยรหัสผ่าน
2) ออกจากการใช้งานโปรแกรม หรือการให้บริการเครือข่าย เมื่อไม่มีความจำเป็นต้องใช้งานอีกต่อไป
3) การรักษาความปลอดภัยคอมพิวเตอร์หรืออุปกรณ์มือถือจากการใช้งานไม่ได้รับอนุญาต โดยล็อคกุญแจ หรือการใส่รหัสผ่าน เมื่อไม่ใช้งาน

นโยบาย Clear-desk-Clear-screen ต้องถูกนำมาใช้ อย่างเหมาะสมกับ ประเภทของข้อมูล, ข้อกำหนดของกฎหมายและสัญญา และความเสี่ยงอื่นๆ ที่เกี่ยวข้อง รวมทั้งวัฒนธรรมของคณะฯ โดยมีแนวทางต่อไปนี้ควรได้รับการพิจารณา

1) ข้อมูลทางการดำเนินงานที่สำคัญหรือสำคัญเช่น บนกระดาษหรือบนสื่อจัดเก็บข้อมูลอิเล็กทรอนิกส์ ต้องถูกจัดเก็บอย่างปลอดภัย (เช่น ในตู้เซฟ ตู้ หรือสถานที่จัดเก็บอื่นๆ ที่ปลอดภัย) เมื่อไม่จำเป็นต้องใช้ โดยเฉพาะอย่างยิ่งในเวลาที่ไม่มีคนอยู่ในสำนักงาน เช่นเวลาพัก หรือเลิกงาน เป็นต้น
2) อุปกรณ์คอมพิวเตอร์ที่ไม่ได้ใช้งาน ต้องถูก log-off หรือ lock หน้าจอหรือคีย์บอร์ด ด้วยรหัสผ่าน, token หรือวิธีการพิสูจน์ตัวตนอื่นๆ
3) ต้องป้องกันการใช้งาน เครื่องสำเนาเอกสาร แฟกซ์ สแกนเนอร์ กล้องดิจิตอล โดยไม่ได้รับอนุญาต
4) สื่อที่มีข้อมูลที่สำคัญ ตามที่มีการกำหนดไว้ ต้องมีการนำออกจากเครื่องพิมพ์ทันทีหลังจากที่ใช้งาน

5) นโยบาย Clear-desk-clear-screen จะช่วยลดความเสี่ยงของการเข้าถึงไม่ได้รับอนุญาต, การสูญเสีย และความเสียหายต่อข้อมูลระหว่างและนอกเวลาทำงานปกติ ตู้เซฟหรือรูปแบบอื่น ๆ ของสิ่งอำนวยความสะดวกการจัดเก็บข้อมูลที่เชื่อถือได้ นอกจากนี้ยังอาจปกป้องข้อมูลที่เก็บไว้ในนั้น จากภัยพิบัติ เช่น ไฟไหม้ แผ่นดินไหวน้ำท่วม หรือการระเบิด
6) พิจารณาการใช้เครื่องพิมพ์ที่มีฟังก์ชั่นรหัส PIN เพื่อให้ผู้สั่งพิมพ์เอกสารเป็นคนเดียวที่จะได้รับงานพิมพ์เมื่ออยู่ที่หน้าเครื่องพิมพ์เท่านั้น