
# นโยบายการใช้งานอุปกรณ์คอมพิวเตอร์พกพา การปฏิบัติงานจากภายนอกคณะฯ และการใช้อุปกรณ์คอมพิวเตอร์ส่วนตัวในการปฏิบัติงาน Mobile Device, Teleworking and BYOD Policy

## คณะแพทยศาสตร์ มหาวิทยาลัยเชียงใหม่

รหัสเอกสาร : ISMS-PL-I-007
ฉบับที่ : 2.0
ประเภทเอกสาร : เอกสารภายใน

**สารบัญ**

# การควบคุมเอกสาร

## การอนุมัติใช้เอกสาร

เอกสารนี้ผ่านการทบทวนและอนุมัติโดย:

| จัดเตรียมเอกสารโดย | ทบทวนเอกสารโดย | อนุมัติเอกสารโดย |
|---|---|---|
| (นางสาวอลิศา นิ่มวรพันธุ์)<br>คณะทำงานระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ | (นางอัจฉราภรณ์ อังศุรัตนเวช)<br>ผู้บริหารระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ | (ศาสตราจารย์ (เชี่ยวชาญพิเศษ) นายแพทย์บรรณกิจ โลจนาภิวัฒน์)<br>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 |
| | | | |
| | | | |
| | | | |

# นโยบายการใช้งานอุปกรณ์คอมพิวเตอร์พกพา การปฏิบัติงานจากภายนอกคณะฯ และการใช้อุปกรณ์คอมพิวเตอร์ส่วนตัวในการปฏิบัติงาน (Mobile Device, Teleworking and BYOD Policy)

## 1. บทนำ

### 1.1 วัตถุประสงค์

เพื่อกำหนดแนวทางการใช้งานอุปกรณ์คอมพิวเตอร์พกพา การปฏิบัติงานจากภายนอกคณะฯ และการใช้อุปกรณ์คอมพิวเตอร์ส่วนตัวในการปฏิบัติงานให้เป็นไปอย่างมั่นคงปลอดภัย และเพื่อเป็นการป้องกันมิให้เกิดการรั่วไหลหรือสูญหายของข้อมูลของคณะฯจากการใช้อุปกรณ์คอมพิวเตอร์พกพา การปฏิบัติงานจากภายนอก และการใช้อุปกรณ์คอมพิวเตอร์ส่วนตัวในการปฏิบัติงาน

### 1.2 ขอบเขต

นโยบายนี้ครอบคลุมถึงการใช้งานอุปกรณ์คอมพิวเตอร์พกพา การปฏิบัติงานจากภายนอกคณะฯ และการใช้อุปกรณ์คอมพิวเตอร์ส่วนตัวในการปฏิบัติงานของพนักงานประจำ พนักงานชั่วคราว คู่สัญญา คู่ค้า ที่ปรึกษา บุคคลภายนอก หรือผู้ใดก็ตามที่ได้รับอนุญาตให้เป็นผู้ใช้งานข้อมูล ระบบเทคโนโลยีสารสนเทศ และทรัพย์สินอื่นๆ ที่เกี่ยวข้องกับระบบเทคโนโลยีสารสนเทศของคณะฯ ภายใต้ขอบเขตการดำเนินการของระบบ ISMS

### 1.3 คำจำกัดความ

| คำ | ความหมาย |
|---|---|
| คณะฯ | คณะแพทยศาสตร์ มหาวิทยาลัยเชียงใหม่ |
| Management Representative (MR) | ตัวแทนฝ่ายบริหารระบบมาตรฐาน ในที่นี้ได้แก่ ISMR หรือ ISMA |
| ISMR | Information Security Management Representative |
| ISMA | Information Security Management Assistance |
| DC | ศูนย์คอมพิวเตอร์แม่ข่ายหลัก |
| DR Site | ศูนย์คอมพิวเตอร์แม่ข่ายสำรอง |

## 2. นโยบาย

### 2.1 การใช้อุปกรณ์คอมพิวเตอร์พกพา

**2.1.1** ผู้ใช้งานต้องปฏิบัติตามนโยบายด้านความมั่นคงปลอดภัยของคณะฯอย่างเคร่งครัด เมื่อมีการใช้งานเครื่องคอมพิวเตอร์พกพา หรืออุปกรณ์คอมพิวเตอร์พกพาอื่นๆ ซึ่งนโยบายเหล่านั้นได้แก่ นโยบายฉบับนี้, Information Classification and Handling Policy และ Acceptable Use Policy อุปกรณ์คอมพิวเตอร์พกพาที่กำหนดในนโยบายนี้หมายรวมถึงอุปกรณ์คอมพิวเตอร์พกพาใดๆ ที่ใช้ในการเชื่อมต่อเข้าสู่ระบบเครือข่าย และ/หรือ ที่ใช้ในการเก็บรักษาข้อมูลของคณะฯ อันได้แก่

- อุปกรณ์มือถือ (ออแกไนเซอร์ส่วนตัว พีดีเอ พ๊อคเก็ตพีซี เป็นต้น)
- สมาร์ทโฟน โทรศัพท์เคลื่อนที่ และ แท็บเล็ตพีซี
- Thumb-Drive และ External Hard disk

**2.1.2** อุปกรณ์คอมพิวเตอร์พกพาเหล่านี้ต้องได้รับการตรวจสอบ เพื่อให้มั่นใจว่าปราศจากซอฟต์แวร์ที่ไม่ได้รับอนุญาต ไวรัสคอมพิวเตอร์ หรือโปรแกรมมุ่งร้ายต่าง ๆ ก่อนที่จะได้รับอนุญาตให้เชื่อมต่อเข้าสู่ระบบเครือข่ายของคณะฯ

**2.1.3** ผู้ใช้งานอุปกรณ์คอมพิวเตอร์พกพาต้องทำการปกป้อง อุปกรณ์ และข้อมูลที่อยู่ในอุปกรณ์เหล่านั้นอย่างเหมาะสม

**2.1.4** ผู้ใช้งานคอมพิวเตอร์พกพาต้องมีการปกป้องทางกายภาพของอุปกรณ์คอมพิวเตอร์พกพาเหล่านั้นอย่างเหมาะสม

**2.1.5** การติดตั้งซอฟต์แวร์ในอุปกรณ์คอมพิวเตอร์พกพาต้องเป็นไปตามที่คณะฯกำหนดเท่านั้น

**2.1.6** อุปกรณ์คอมพิวเตอร์พกพาต้องได้รับการปรับปรุงเวอร์ชั่นและติดตั้ง Patch ของอุปกรณ์คอมพิวเตอร์พกพาเหล่านั้นให้ทันสมัยอยู่เสมอ

**2.1.7** คณะฯไม่อนุญาตให้ทำการ Jailbreak (สำหรับ iOS) หรือ Rooted (สำหรับ Android) ในอุปกรณ์สมาร์ทโฟน

**2.1.8** อุปกรณ์คอมพิวเตอร์พกพาต้องได้รับการติดตั้งโปรแกรมป้องกันไวรัส และต้องได้รับการปรับปรุงให้ทันสมัยอยู่เสมอ

**2.1.9** ข้อมูลที่เป็นความลับหรือมีความอ่อนไหวสูงที่อยู่บนอุปกรณ์คอมพิวเตอร์พกพาต้องได้รับการเข้ารหัสข้อมูลตาม Encryption Standard ของคณะฯเพื่อป้องกันข้อมูลไม่ให้ข้อมูลรั่วไหลไปยังบุคคลที่ไม่ได้รับอนุญาตให้เข้าถึงข้อมูลเหล่านั้นได้

**2.1.10** อุปกรณ์คอมพิวเตอร์พกพาต้องได้รับการป้องกันการเข้าถึงเครื่องอุปกรณ์คอมพิวเตอร์พกพาเหล่านั้นโดยการกำหนดรหัสผ่านที่มั่นคงปลอดภัย

**2.1.11** อุปกรณ์คอมพิวเตอร์พกพาต้องได้รับการสำรองข้อมูลที่มีความสำคัญที่ถูกจัดเก็บไว้บนอุปกรณ์เหล่านั้นอย่างสม่ำเสมอ

**2.2 การปฏิบัติงานจากภายนอกคณะฯ**

**2.2.1** พนักงานต้องหลีกเลี่ยงการปฏิบัติงานจากภายนอกคณะฯ (Teleworking หรือ Telecommuting) ไม่ว่าการปฏิบัติงานนั้นจะกระทำโดยใช้อุปกรณ์คอมพิวเตอร์ของคณะฯ หรืออุปกรณ์คอมพิวเตอร์ส่วนตัว เว้นแต่จะได้รับอนุญาตจากหัวหน้างานเท่านั้น

**2.2.2** เปิดการใช้งานซอฟต์แวร์หรืออุปกรณ์ประเภท Virtual Private Network หรือเทคโนโลยีอื่นๆ เพื่อปกป้องการเชื่อมต่อระหว่างสถานที่ปฏิบัติงานภายนอกและเครือข่ายภายในของคณะฯ

**2.2.3** ควรใช้กระบวนการพิสูจน์ตัวตน ที่สามารถตรวจสอบตัวตนผู้ใช้งานด้วยวิธีการตรวจสอบตั้งแต่ 2 ประเภทขึ้นไป (Two factors authentication) เช่น One-time Password (OTP), Tokens หรือ Biometric Devices เป็นต้น

**2.2.4** เข้ารหัสข้อมูลที่ถูกนำไปใช้ในการปฏิบัติงานนอกสถานที่ หรือการปฏิบัติงานจากภายนอกคณะฯ ตาม Encryption Standard ของคณะฯ

**2.2.5** พนักงานที่ได้รับอนุญาตให้ปฏิบัติงานจากภายนอกคณะฯ ต้องใช้ความระมัดระวังมากเป็นพิเศษ เพื่อปกป้องอุปกรณ์คอมพิวเตอร์พกพา รวมถึงข้อมูลที่อยู่ในอุปกรณ์เหล่านั้นมิให้ถูกล่วงละเมิดโดยบุคคลที่ไม่ได้รับอนุญาต ซึ่งรวมถึงสมาชิกในครอบครัวของพนักงานด้วย

**2.2.6** พนักงานต้องได้รับการฝึกอบรม หรือได้รับคำแนะนำอย่างเหมาะสมเกี่ยวกับการเข้าถึงระบบจากระยะไกล และการปกป้องข้อมูลที่ถูกใช้งาน หรือถูกเก็บรักษาอยู่ภายนอกสถานที่อันเนื่องมาจากการปฏิบัติงานจากภายนอกคณะฯ

**2.2.7** สถานที่ปฏิบัติงานจากภายนอกคณะฯต้องมีความปลอดภัยทางด้านกายภาพทั้งในส่วนของตัวอาคารและสภาพแวดล้อม

**2.2.8** การสื่อสารระหว่างสถานที่ในการปฏิบัติงานจากภายนอกคณะฯกับองค์กรใหญ่ต้องเป็นไปอย่างมั่นคงปลอดภัย

**2.2.9** เปิดการใช้งาน Virtual Desktop ในการปฏิบัติงานจากภายนอกคณะฯ เพื่อป้องกันข้อมูลที่ถูกเก็บบนเครื่องรั่วไหลไปยังบุคคลที่ไม่ได้รับอนุญาต

**2.2.10** การปฏิบัติงานจากภายนอกคณะฯ พนักงานต้องป้องกันการเข้าถึงข้อมูลของทางคณะฯจากบุคคลที่ไม่เกี่ยวข้อง เช่น เพื่อน หรือ บุคคลในครอบครัว

**2.2.11** การใช้งานเครือข่ายไร้สายที่บ้านของพนักงาน ต้องเป็นไปอย่างมั่นคงปลอดภัย โดยต้องมีการเข้ารหัสสัญญาณและป้องกันการเข้าถึงจากบุคคลที่ไม่เกี่ยวข้อง (การเข้ารหัสของ Wi-fi ขั้นต่ำเป็น WPA2)

**2.2.12** งานที่พนักงานทำให้คณะฯ จากระยะไกลในอุปกรณ์คอมพิวเตอร์ส่วนตัวของพนักงานจะถือว่าเป็นทรัพย์สินทางปัญญาของคณะฯ

**2.2.13** พนักงานต้องยินยอมให้คณะฯตรวจสอบอุปกรณ์คอมพิวเตอร์ส่วนตัวของพนักงานเมื่อมีการร้องขอจากทางคณะฯ ทั้งนี้เพื่อความปลอดภัยของอุปกรณ์คอมพิวเตอร์ส่วนตัวที่ใช้ในการเข้าถึงข้อมูลของทางคณะฯ

**2.2.14** ซอฟต์แวร์ที่ติดตั้งในอุปกรณ์คอมพิวเตอร์ส่วนตัวของพนักงานถือว่าเป็นซอฟต์แวร์ส่วนบุคคลของพนักงานเอง คณะฯ จะไม่ถือว่าเป็น License ของทางคณะฯ

**2.2.15** อุปกรณ์คอมพิวเตอร์ส่วนตัวที่พนักงานใช้ในการปฏิบัติงานจากภายนอกคณะฯต้องได้รับการเปิดการใช้งาน Personal Firewall และติดตั้งและเปิดการใช้งานโปรแกรม Antivirus ที่ถูกปรับปรุงให้ทันสมัยอยู่เสมอ

**2.2.16** อุปกรณ์คอมพิวเตอร์ที่นำออกไปใช้งานนอกคณะฯ จำเป็นที่จะต้องมีการระบุสถานที่ Geolocation เพื่อการระบุพิกัด สถานที่ ประเทศที่ไม่เป็นสถานที่ต้องสงสัยว่าจะมีการโจมตีทางไซเบอร์มายังคณะฯ และเป็นการระบุสถานที่ที่ใช้งานอุปกรณ์นั้นๆ

## 2.3 การใช้อุปกรณ์คอมพิวเตอร์ส่วนตัวในการปฏิบัติงาน

**2.3.1** งานเทคโนโลยีสารสนเทศมีสิทธิ์ในการปฏิเสธการเข้าใช้งานจากอุปกรณ์คอมพิวเตอร์ส่วนตัวของพนักงานในการเข้าถึงข้อมูลและระบบของทางคณะฯ หากคณะฯ พบว่าอุปกรณ์ดังกล่าวอาจก่อให้เกิดความเสี่ยงต่อข้อมูล ระบบ พนักงาน และผู้รับบริการของคณะฯ

**2.3.2** งานเทคโนโลยีสารสนเทศมีสิทธิ์ในการติดตั้งโปรแกรมทำลายข้อมูล (Self-Destruct) บนอุปกรณ์คอมพิวเตอร์ส่วนตัวของพนักงานที่นำมาใช้ปฏิบัติงาน โดยคณะฯ อาจจะมีการสั่งลบข้อมูลบนอุปกรณ์คอมพิวเตอร์ส่วนตัวของพนักงานในกรณีที่เกิดเหตุการณ์ที่ทำให้เกิดการรั่วไหลหรือความไม่ปลอดภัยของข้อมูล

**2.3.3** คณะฯมีสิทธิ์ที่จะตรวจสอบอุปกรณ์คอมพิวเตอร์ส่วนตัวที่มีการใช้งานกับ Infrastructure ของทางคณะฯ หากพนักงานปฏิเสธการตรวจสอบ ทางคณะฯจะทำการยกเลิกสิทธิ์ในการเข้าถึง รวมทั้ง User ID และ Password ของพนักงาน

**2.3.4** ก่อนที่พนักงานจะนำอุปกรณ์คอมพิวเตอร์ส่วนตัวมาใช้งานภายในคณะฯ พนักงานจะต้องได้รับการอนุมัติและลงทะเบียนอุปกรณ์คอมพิวเตอร์ส่วนตัวนั้นกับงานเทคโนโลยีสารสนเทศก่อน โดยที่พนักงานจะต้องปฏิบัติตาม Information Classification and Handling Policy ของทางคณะฯ อย่างเคร่งครัด เพื่อความมั่นคงปลอดภัยสารสนเทศของคณะฯ

**2.3.5** พนักงานที่ต้องการเข้าถึงข้อมูลภายในคณะฯจากเครือข่ายที่ไม่ใช่เครือข่ายของทางคณะฯจะต้องทำการติดตั้งและเปิดการใช้งาน Personal Firewall และ Antivirus รวมถึงซอฟต์แวร์อื่น ๆ ที่จำเป็นที่ถูกกำหนดโดยงานเทคโนโลยีสารสนเทศ

**2.3.6** อุปกรณ์คอมพิวเตอร์ส่วนตัวทั้งหมดที่เข้าถึงเครือข่ายของคณะฯจะสามารถถูกตรวจสอบโดยคณะฯได้ว่าได้รับอนุญาตจากทางคณะฯ แล้วหรือไม่ หากคณะฯพบว่าเป็นอุปกรณ์คอมพิวเตอร์ส่วนตัวที่ไม่ได้รับอนุญาตและพยายามที่จะเข้าถึงเครือข่ายของทางคณะฯจะถูกปฏิเสธการเข้าถึงทันที

**2.3.7** อุปกรณ์คอมพิวเตอร์ส่วนตัวจะสามารถเข้าถึงเครือข่ายและข้อมูลของทางคณะฯ โดยการใช้งานผ่าน SSL/TLS VPN โดยข้อมูลการเข้าถึง SSL/TLS VPN Portal ของคณะฯจะถูกส่งให้พนักงานเมื่อได้รับอนุญาตจากงานเทคโนโลยีสารสนเทศ

**2.3.8** พนักงานที่ใช้อุปกรณ์คอมพิวเตอร์ส่วนตัวในการปฏิบัติงานต้องปฏิบัติตาม Information Classification and Handling Policy ของคณะฯ อย่างเคร่งครัด

**2.3.9** อุปกรณ์คอมพิวเตอร์ส่วนตัวต้องได้รับการป้องกันการเข้าถึงโดยใช้รหัสผ่าน และข้อมูลที่อยู่ในอุปกรณ์คอมพิวเตอร์ส่วนตัวต้องมีการเข้ารหัสข้อมูล โดยพนักงานสามารถดูมาตรฐานการเข้ารหัสข้อมูลได้จาก Encryption Standard

**2.3.10** พนักงานที่ใช้อุปกรณ์คอมพิวเตอร์ส่วนตัวต้องเก็บรักษารหัสผ่านโดยไม่ให้บุคคลอื่นทราบ โดยเฉพาะบุคคลภายในครอบครัวหากมีการใช้อุปกรณ์คอมพิวเตอร์ส่วนตัวทำงานที่บ้าน

**2.3.11** พนักงานที่มีการใช้งานอุปกรณ์คอมพิวเตอร์ส่วนตัวต้องมีการป้องกันทางด้านกายภาพของเครื่องทั้งในขณะที่ใช้งานและในขณะที่มีการเคลื่อนย้ายอุปกรณ์ โดยการป้องกันเหล่านี้รวมถึงการป้องกันด้วยรหัสผ่าน การเข้ารหัสข้อมูล และการป้องกันทางกายภาพของอุปกรณ์คอมพิวเตอร์ส่วนตัวที่มีข้อมูลของทางคณะฯ โดยหากอุปกรณ์คอมพิวเตอร์ส่วนตัวมีการ Synchronize กับอุปกรณ์อื่น ๆ อุปกรณ์นั้น ๆ จะต้องได้รับการติดตั้งและเปิดการใช้งาน Antivirus และ Anti-malware และซอฟต์แวร์อื่น ๆ ที่ถูกกำหนดให้มีการติดตั้งโดยงานเทคโนโลยีสารสนเทศ

**2.3.12** Antivirus signature บนอุปกรณ์คอมพิวเตอร์ส่วนตัวต้องได้รับการปรับปรุงให้ทันสมัยอยู่เสมอ

**2.3.13** รหัสผ่านและข้อมูลความลับอื่นๆ ที่ถูกกำหนดโดยคณะฯตาม Information Classification and Handling Policy ต้องได้รับการเข้ารหัสบนอุปกรณ์คอมพิวเตอร์ส่วนตัว