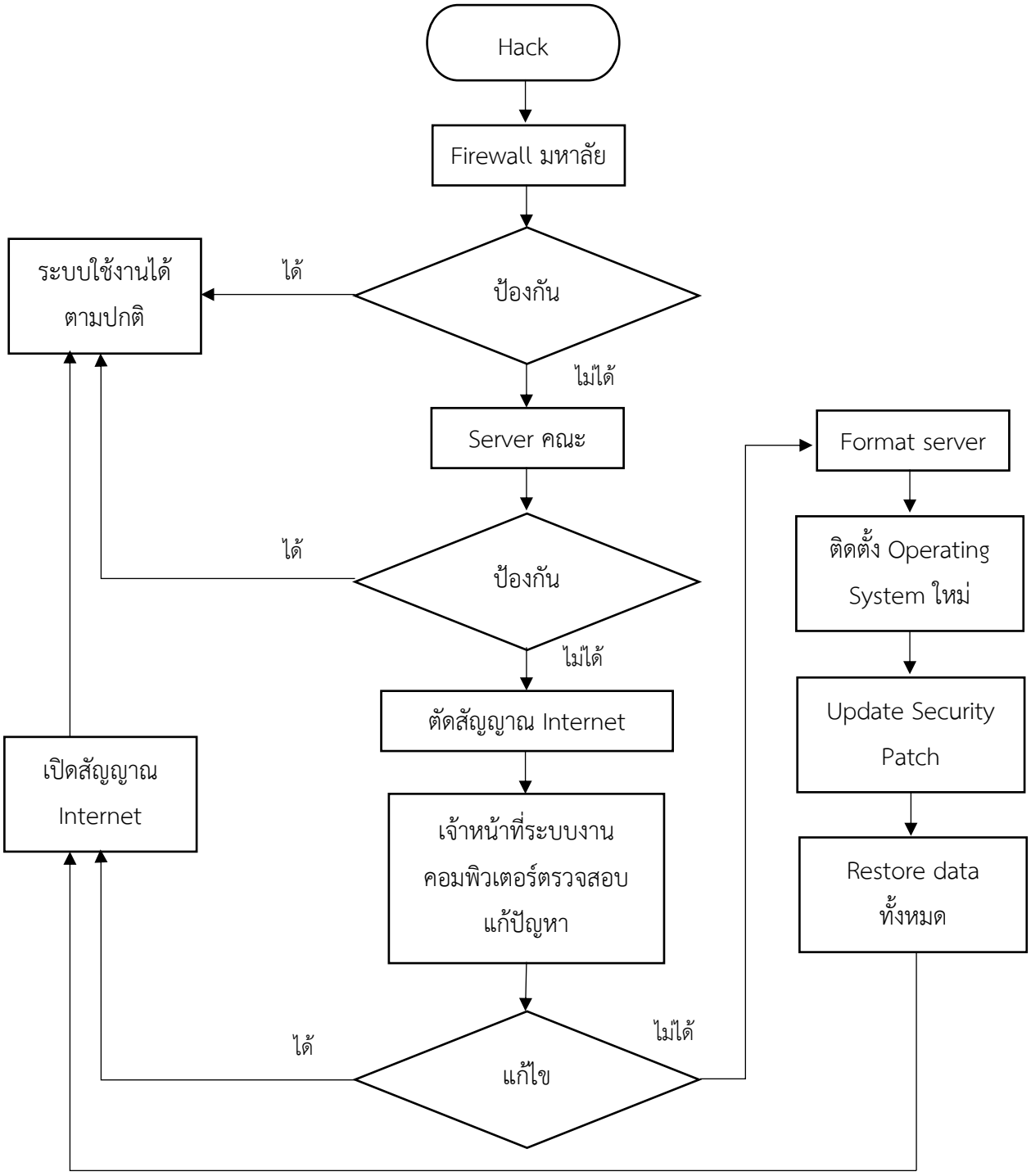
Mahidol University
Faculty of Nursing

Cyber Security plan
และแนวปฏิบัติ
งานเทคโนโลยีสารสนเทศ
ปีงบประมาณ 2564-2567

Cyber security plan และแนวปฏิบัติ

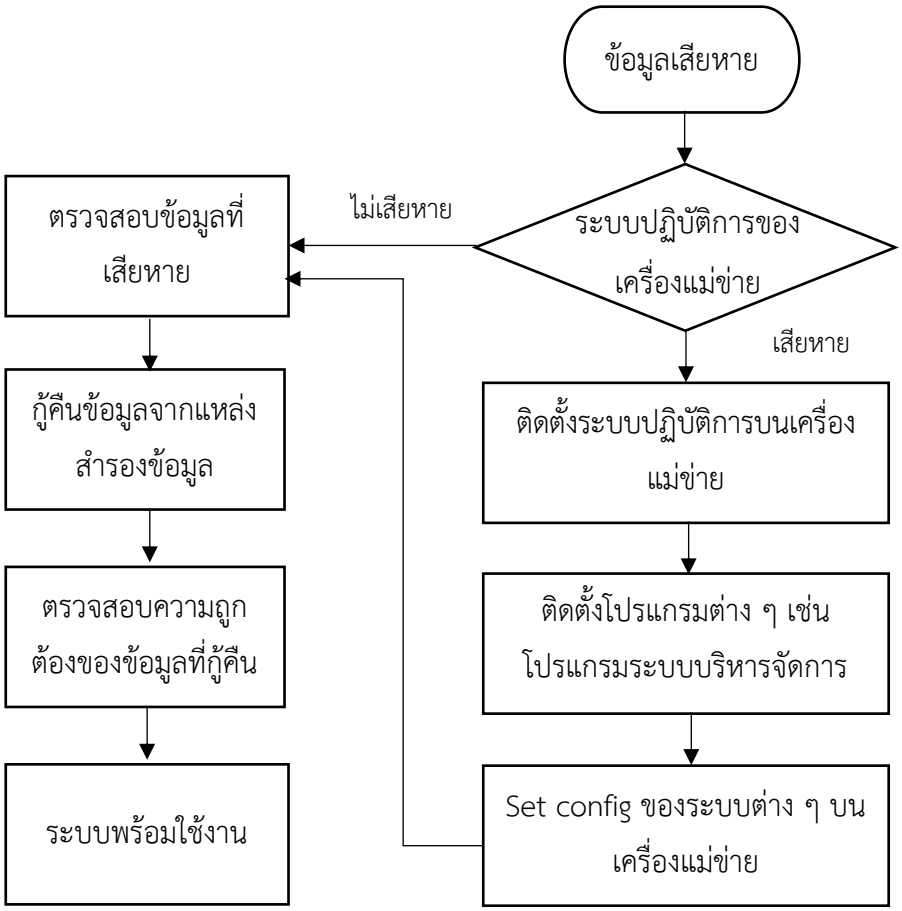
งานเทคโนโลยีสารสนเทศ คณะพยาบาลศาสตร์ มหาวิทยาลัยมหิดล

<u>กรณีถูกโจมตีทางไซเบอร์</u>



แผนผัง 1 แสดง Cyber Security plan กรณีถูกโจมตีทางไซเบอร์

<u>กรณีกู้คืนข้อมูล</u>



แผนผัง 2 แสดง Cyber Security plan กรณีกู้คืนข้อมูล

ผู้รับผิดชอบ

- ผู้ช่วยคณบดีฝ่ายนวัตกรรมการศึกษาและสารสนเทศ ควบคุม
- เจ้าหน้าที่ระบบงานคอมพิวเตอร์ ตรวจสอบ แก้ปัญหา

แนวปฏิบัติ

เมื่อมีการ Hack เข้าสู่ระบบ จะมี Firewall ของมหาวิทยาลัยทำหน้าที่ปิดกั้นและป้องกันอันตรายในเบื้องต้น หาก Firewall มหาวิทยาลัย ไม่สามารถปิดกั้นอันตรายทางไซเบอร์ได้ จะมี Server ของคณะที่มีระบบความปลอดภัยที่ทำการอัพเดทอัตโนมัติอยู่เสมอ และทำการติดตั้งโดยเจ้าหน้าที่ระบบงานคอมพิวเตอร์ทุกสัปดาห์ หาก Server ของคณะไม่สามารถปิดกั้นอันตรายได้ Internet ภายในคณะ จะถูกตัดสัญญาณ เจ้าหน้าที่ระบบงานคอมพิวเตอร์จะดำเนินการตรวจสอบ และแก้ไขปัญหาที่เกิดขึ้น เมื่อแก้ไขได้แล้วจึงจะดำเนินการเปิดสัญญาณ internet ตามปกติ หากไม่สามารถแก้ไขได้จะดำเนินการแก้ปัญหา ตามลำดับ ดังนี้

1. Format server
2. ติดตั้ง Operating System ใหม่
3. Update Security Patch
4. Restore data ทั้งหมด

เพื่อให้ระบบความปลอดภัยของ server คณะมีประสิทธิภาพในการป้องกันความปลอดภัยทางไซเบอร์ จึงมีขั้นตอนการป้องกัน ดังนี้

1. ติดตั้ง Firewall on windows
2. Update patch ของ Operating System (OS) โดยจะอัพเดทอัตโนมัติ และทำการติดตั้งโดยเจ้าหน้าที่ระบบงานคอมพิวเตอร์ทุกวันศุกร์ของสัปดาห์
3. ESET for Server update pattern Virus โดยจะอัพเดทอัตโนมัติ

เพื่อป้องกันผลกระทบจากการถูกโจมตีทางไซเบอร์ ได้มีแนวปฏิบัติเพื่อสำรองข้อมูลสำคัญ โดยมีการสำรองข้อมูลสำคัญไว้ที่เครื่องของผู้ปฏิบัติงานที่รับผิดชอบงานนั้นๆ เช่น Webmaster, E-learning Administrator, Programmer ระบบสารสนเทศ นอกจากสำรองข้อมูลในเครื่องของผู้ปฏิบัติงาน ได้มีการสำรองข้อมูลเพิ่มเติมไปยัง External Hard disk ที่กำหนด และ Cloud storage ด้วย โดยจะสำรองข้อมูลทุกครั้งที่มีการแก้ไข ส่วน Database มีการสำรองทุกวันศุกร์

ในกรณีเกิดการสูญเสียข้อมูลจากการ Hack เจ้าหน้าที่ระบบงานคอมพิวเตอร์จะดำเนินการกู้คืนข้อมูล โดยพิจารณาจากความเสียหายของข้อมูลที่เกิดขึ้น แบ่งออกเป็น 2 ประเภท คือ

1. ข้อมูลเสียหายแต่ระบบปฏิบัติการของเครื่องแม่ข่ายไม่เสียหาย
   1.1 ตรวจสอบข้อมูลที่เสียหายว่าเป็นข้อมูลใดบ้าง

1.2 เมื่อระบุข้อมูลที่เสียหายได้แล้ว ทำการกู้คืนข้อมูล จากแหล่งข้อมูลสำรอง (backup hard disk/cloud storage)

1.3 ตรวจสอบความถูกต้องของข้อมูลที่กู้คืน

1.4 ระบบพร้อมใช้งาน

2. ระบบปฏิบัติการของเครื่องแม่ข่ายเสียหายไม่สามารถทำงานได้

2.1 ติดตั้งระบบปฏิบัติการบนเครื่องแม่ข่าย

2.2 หลังจากติดตั้งระบบปฏิบัติการเสร็จ ติดตั้งโปรแกรมต่าง ๆ เช่น โปรแกรมระบบบริหารจัดการฐานข้อมูล, โปรแกรมป้องกัน Virus

2.3 Set config ของระบบต่าง ๆ บนเครื่องแม่ข่าย เช่น website หลัก, Virtual Directory เป็นต้น

2.4 ทำการกู้คืนข้อมูล จากแหล่งข้อมูลสำรอง (backup hard disk/cloud storage)

2.5 ตรวจสอบความถูกต้องของข้อมูลที่กู้คืน

2.6 ระบบพร้อมใช้งาน