
# รหัสเอกสาร : SD-ISMS-01

# นโยบายและแนวปฏิบัติ
# ในการรักษาความมั่นคงปลอดภัยสารสนเทศ

**แก้ไขครั้งที่ 01** **เริ่มใช้วันที่ 10 มีนาคม 2566**

**อนุมัติโดย :** .....

( รศ.นพ.ดิลก ภิยโยทัย )

คณบดี

**ประวัติการแก้ไข**

## ประวัติการแก้ไข

| แก้ไขครั้งที่ | DAR No | เริ่มใช้วันที่ | รายละเอียด |
|---|---|---|---|
| 01 | 13/66 | 10 มีนาคม 2566 | - ปรับเปลี่ยนรายละเอียดเรื่องการเปลี่ยนรหัสผ่านของผู้ดูแลระบบ ข้อ 3.3.2.7 หน้า 18<br>- ปรับเปลี่ยนรายละเอียดเรื่องการจำกัดระยะเวลาการเชื่อมต่อระบบสารสนเทศ ข้อ 3.4.1.2 หน้า 18<br>- ปรับเปลี่ยนรายละเอียดเรื่องมาตรการการเข้ารหัสข้อมูล ข้อ 4.1 หน้า 20<br>- ปรับเปลี่ยนรายละเอียดเรื่อง Clock Synchronization ข้อ 6.4.6 หน้า 27<br>- ปรับเปลี่ยนรายละเอียดเรื่องการแบ่งแยกเครือข่าย ข้อ 7.1.3 หน้า 32 |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |

# สารบัญ

# บททั่วไป

**1) หลักการและเหตุผล**

ปัจจุบันมีการนำเทคโนโลยีสารสนเทศและการสื่อสารมาใช้เป็นเครื่องมือสำคัญกันอย่างแพร่หลาย เพื่อให้ได้มาซึ่งข้อมูลสารสนเทศที่เป็นประโยชน์ต่อการบริหาร การดำเนินกิจกรรมภายในองค์กรที่สะดวก รวดเร็ว ขณะเดียวกัน องค์กรอาจประสบปัญหาความไม่น่าเชื่อถือของสารสนเทศได้อันมีสาเหตุมาจากการใช้งานที่ไม่เหมาะสม ความไม่ทันสมัย ความไม่ถูกต้องครบถ้วนเพียงพอ ซึ่งอาจนำไปสู่ผลเสียต่อการดำเนินงานและชื่อเสียงขององค์กรเป็นอย่างมาก ดังนั้นการพัฒนาระบบสารสนเทศโดยคำนึงถึงความมั่นคงปลอดภัยของข้อมูลสารสนเทศจึงเป็นเรื่องที่มีความสำคัญต่อองค์กรอย่างมาก โดยองค์ประกอบหลัก ของความมั่นคงปลอดภัยของข้อมูลสารสนเทศประกอบด้วย CIA ได้แก่ Confidentiality (การรักษาความลับ) ข้อมูลระบบสารสนเทศจะต้องเข้าถึงได้โดยผู้มีสิทธิ์และได้รับอนุญาตเท่านั้น ดังนั้นจึงต้องมีมาตรการในการรักษาความมั่นคงปลอดภัย ที่เพียงพอในการรักษาความลับของข้อมูลและระบบสารสนเทศ, Integrity (ความถูกต้องความสมบูรณ์) รวมถึง ความถูกต้องครบถ้วนของข้อมูล, Availability (ความพร้อมใช้) ระบบสารสนเทศจะถูกเข้าใช้หรือเรียกใช้งานได้อย่างราบรื่น โดยผู้ใช้ระบบที่ได้รับอนุญาตเท่านั้น

งานเทคโนโลยีทางการศึกษา คณะแพทยศาสตร์ มหาวิทยาลัยธรรมศาสตร์ ได้เล็งเห็นความสำคัญในการ พัฒนาระบบงานให้มีการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศขึ้นโดยการประยุกต์ใช้ข้อกำหนดมาตรฐานสากล ISO/IEC 27001 เป็นกรอบ ในการดำเนินงาน เพื่อให้การใช้งานระบบสารสนเทศมีความน่าเชื่อถือ ปลอดภัย และสามารถให้บริการระบบสารสนเทศได้อย่างต่อเนื่อง ลดความเสี่ยงจากภัยคุกคามต่าง ๆ ในระบบสารสนเทศ ตลอดจนมีการบริหารจัดการอย่างเป็นระบบ เพื่อให้บุคลากรในคณะ นักศึกษา และบุคคลภายนอกมีความมั่นใจในการใช้งานระบบสารสนเทศของคณะแพทยศาสตร์ต่อไป

**2) วัตถุประสงค์**

1.2.1 เพื่อกำหนดแนวปฏิบัติด้านการรักษาความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ สร้างความน่าเชื่อถือมั่นคง และปลอดภัย ในระบบสารสนเทศภายในของงานเทคโนโลยีทางการศึกษา คณะแพทยศาสตร์ มหาวิทยาลัยธรรมศาสตร์

1.2.2 เพื่อสร้างความเข้าใจ และความตระหนักในการใช้งานระบบสารสนเทศอย่างปลอดภัยสำหรับผู้ปฏิบัติงานที่เป็นบุคลากรภายใน ผู้รับจ้างภายนอกที่ปฏิบัติหน้าที่ในงานเทคโนโลยีทางการศึกษา คณะแพทยศาสตร์ มหาวิทยาลัยธรรมศาสตร์

1.2.3 เพื่อกำหนดแนวปฏิบัติสำหรับผู้ควบคุมระบบสารสนเทศ (Admin) เพื่อให้มั่นใจได้ว่าระบบได้รับการเฝ้าระวังติดตามความมั่นคงปลอดภัย สอดคล้องตามมาตรฐาน ISO/IEC 27001

**3) บทบังคับใช้**

นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยสารสนเทศฉบับนี้ให้มีผลบังคับใช้กับผู้บริหาร ผู้ใช้งานระบบสารสนเทศ ผู้ทำหน้าที่ดูแลทรัพย์สิน ผู้ใช้ทรัพย์สิน และผู้มีส่วนเกี่ยวข้องในระบบสารสนเทศ รวมทั้งบุคคลภายนอกที่ดำเนินการเกี่ยวข้องกับระบบสารสนเทศขององค์กร จะต้องให้ความร่วมมือในการปฏิบัติตามนโยบายนี้ ผู้ฝ่าฝืนไม่ปฏิบัติตามนโยบายนี้มีความผิดและจะต้องได้รับการดำเนินการตามระเบียบขององค์กร

**4) การเผยแพร่ และทบทวนนโยบาย**

นโยบายการรักษาความมั่นคงปลอดภัยสารสนเทศของงานเทคโนโลยีทางการศึกษา คณะแพทยศาสตร์ มหาวิทยาลัยธรรมศาสตร์ฉบับนี้ จะได้นำออกเผยแพร่โดยการประกาศแจ้งเวียนในระบบสารสนเทศเครือข่ายภายในองค์กร หรือจัดพิมพ์เผยแพร่ อบรมสร้างความตระหนักเพื่อให้บุคลากรในงานเทคโนโลยีทางการศึกษา และบุคลากรในหน่วยงานอื่นๆ ของคณะแพทยศาสตร์ มหาวิทยาลัยธรรมศาสตร์ รวมทั้งบุคคลภายนอกที่เกี่ยวข้อง ได้ทราบและถือปฏิบัติ ตามนโยบายนี้อย่างเคร่งครัด

นโยบายการรักษาความมั่นคงปลอดภัยสารสนเทศนี้กำหนดให้มีการทบทวนอย่างน้อยปีละ 1 ครั้ง หรือเมื่อมีการเปลี่ยนแปลงในระบบสารสนเทศที่มีนัยสำคัญ เพื่อให้มั่นใจว่ามีความถูกต้อง ต่อเนื่อง มีประสิทธิภาพ สอดคล้องกับบริบทและผลการประเมินความเสี่ยงขององค์กร

---

# คำนิยาม

1. **องค์กร** หมายถึง คณะแพทยศาสตร์ มหาวิทยาลัยธรรมศาสตร์
2. **หน่วยงาน** หมายถึง งานเทคโนโลยีทางการศึกษา สำนักงานเลขานุการ
3. **แนวปฏิบัติ** หมายถึง แนวทางที่ต้องปฏิบัติตามเพื่อให้สามารถบรรลุวัตถุประสงค์หรือเป้าหมายของนโยบาย
4. **ผู้ใช้งาน** หมายถึง ผู้บริหารขององค์กร ผู้ดูแลระบบ ผู้รับผิดชอบ ผู้ใช้งานทั่วไป อันได้แก่
   - 4.1 ผู้บริหารสูงสุด หมายถึง คณบดีคณะแพทยศาสตร์
   - 4.2 ผู้บริหารระดับสูงของหน่วยงาน หมายถึง ผู้ช่วยคณบดีฝ่ายงานเทคโนโลยีทางการศึกษา
   - 4.3 ผู้ดูแลระบบ หมายถึง เจ้าหน้าที่ที่ได้รับมอบหมายให้มีหน้าที่ดูแลรักษาระบบสารสนเทศหรือ ระบบเครือข่าย หรืออุปกรณ์ในระบบสารสนเทศ
   - 4.4 ผู้พัฒนาระบบ หมายถึง เจ้าหน้าที่ที่ได้รับมอบหมายให้มีหน้าที่รับผิดชอบพัฒนาระบบแอพพลิเคชั่น
   - 4.5 ผู้ใช้งานระบบ หมายถึง บุคลากรและนักศึกษาของคณะแพทยศาสตร์
   - 4.6 บุคคลภายนอก หมายความว่า บุคคลที่องค์กรอนุญาตให้เข้ามาใช้ระบบเทคโนโลยีสารสนเทศขององค์กรได้ชั่วคราว เพื่อประโยชน์ในการดำเนินงาน รวมถึง พนักงานหรือบริษัทภายนอกที่เข้ามาติดตั้งหรือดูแลรักษาระบบ หรือ ที่ปรึกษา หรือผู้ปฏิบัติงานตามสัญญาจ้าง นักศึกษา
5. **สิทธิของผู้ใช้งาน** หมายถึง สิทธิทั่วไป สิทธิจำเพาะ สิทธิพิเศษ และสิทธิอื่นใดที่เกี่ยวข้องกับระบบสารสนเทศขององค์กร
6. **ทรัพย์สิน** (Asset) หรือ ทรัพย์สินสารสนเทศ หมายถึง สิ่งใดก็ตามที่มีคุณค่าสำหรับองค์กร อันได้แก่
   - 6.1 ระบบเครือข่ายคอมพิวเตอร์ ระบบคอมพิวเตอร์ ระบบงานคอมพิวเตอร์ และระบบสารสนเทศ
   - 6.2 ตัวเครื่องคอมพิวเตอร์ อุปกรณ์คอมพิวเตอร์ เครื่องบันทึกข้อมูล และอุปกรณ์อื่นใด
   - 6.3 ข้อมูลสารสนเทศ ข้อมูลอิเล็กทรอนิกส์ และข้อมูลคอมพิวเตอร์
   - 6.4 บุคลากร
7. **การเข้าถึงหรือควบคุมการใช้งานสารสนเทศ (Access Control)** หมายถึง การอนุญาต การกำหนดสิทธิ์ หรือการมอบอำนาจให้ผู้ใช้งานเข้าถึง หรือใช้งานเครือข่าย หรือระบบสารสนเทศ ทั้งทางอิเล็กทรอนิกส์และทางกายภาพ รวมทั้งการอนุญาตดังกล่าวสำหรับบุคคลภายนอก
8. **ความมั่นคงปลอดภัยด้านสารสนเทศ/ระบบสารสนเทศ (Information Security)** หมายถึง การธำรงไว้ซึ่งความลับ (Confidentiality) ความถูกต้องครบถ้วน (Integrity) และสภาพพร้อมใช้งาน (Availability) ของสารสนเทศ

รวมทั้งคุณสมบัติอื่น ได้แก่ ความถูกต้องแท้จริง (Authenticity) ความรับผิด(Accountability) ห้ามปฏิเสธความรับผิด (Non-repudiation) และความน่าเชื่อถือ (Reliability) และหมายความรวมถึง การป้องกันทรัพย์สินสารสนเทศจากการเข้าถึง ใช้ เปิดเผย ขัดขวาง เปลี่ยนแปลงแก้ไข ทำสูญหาย ทำให้เสียหาย ถูกทำลาย หรือล่วงรู้ โดยมิชอบ

9. **เหตุการณ์ด้านความมั่นคงปลอดภัย (Information Security event)** หมายถึง กรณีที่ระบุการเกิดเหตุการณ์สภาพของบริการหรือเครือข่ายที่แสดงให้เห็นความเป็นไปได้ที่จะเกิดการฝ่าฝืนนโยบายด้านความมั่นคงปลอดภัยหรือมาตรการป้องกันที่ล้มเหลว หรือเหตุการณ์อันไม่อาจรู้ได้ว่าอาจเกี่ยวข้องกับความมั่นคงปลอดภัย
10. **สถานการณ์ความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด (Information Security Incident)** หมายถึง สถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด (Unwanted or Unexpected) ซึ่งอาจทำให้ระบบขององค์กรถูกบุกรุกหรือโจมตี และความมั่นคงปลอดภัยถูกคุกคาม
11. **หน่วยงานภายนอก** หมายถึง องค์กรหรือหน่วยงานที่องค์กรอนุญาตให้มีสิทธิ์ในการเข้าถึงและใช้งานข้อมูลหรือทรัพย์สินต่าง ๆ ของหน่วยงาน โดยจะได้รับสิทธิในการใช้งานตามอำนาจและต้องรับผิดชอบในการรักษาความลับของข้อมูลขององค์กร
12. **ข้อมูลคอมพิวเตอร์** หมายถึง ข้อมูล ข้อความ คำสั่ง ชุดคำสั่ง ที่อยู่ในระบบคอมพิวเตอร์ในสภาพที่ระบบคอมพิวเตอร์อาจประมวลผลได้ และให้ความหมายรวมถึงข้อมูลอิเล็กทรอนิกส์ตาม พระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. 2544 และฉบับแก้ไขเพิ่มเติม (ฉบับที่ 2) พ.ศ. 2551
13. **ข้อมูลจราจรทางคอมพิวเตอร์** หมายถึง ข้อมูลเกี่ยวกับการติดต่อสื่อสารของระบบคอมพิวเตอร์ ซึ่งแสดงถึงแหล่งกำเนิด ต้นทาง ปลายทาง เส้นทาง เวลา วันที่ ปริมาณ ระยะเวลา ชนิดของบริการ หรืออื่นๆ ที่เกี่ยวข้องกับการติดต่อสื่อสารของระบบคอมพิวเตอร์นั้น
14. **สารสนเทศ (Information)** หมายถึง ข้อเท็จจริงที่ได้จากข้อมูลนำมาผ่านการประมวลผล การจัดระเบียบให้ข้อมูลซึ่งอาจอยู่ในรูปของตัวเลข ข้อความ หรือภาพกราฟิก ให้เป็นระบบที่ผู้ใช้สามารถเข้าใจได้ง่ายและสามารถนำไปใช้ประโยชน์ในการบริหาร การวางแผน การตัดสินใจ และอื่น ๆ
15. **ระบบคอมพิวเตอร์** หมายถึง อุปกรณ์หรือชุดอุปกรณ์ของคอมพิวเตอร์ที่เชื่อมการทำงานเข้าด้วยกันโดยไม่มีการกำหนดคำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใด และแนวทางปฏิบัติงานให้อุปกรณ์ หรือชุดอุปกรณ์ทำหน้าที่ประมวลผลข้อมูลโดยอัตโนมัติ
16. **ระบบเครือข่าย (Network System)** หมายถึง ระบบที่สามารถใช้ในงานติดต่อสื่อสารหรือการส่งข้อมูลและสารสนเทศระหว่างระบบเทคโนโลยีสารสนเทศต่าง ๆ ขององค์กรได้ เช่น ระบบแลน (LAN), ระบบอินทราเน็ต (Intranet), ระบบอินเตอร์เน็ต (Internet)

17. **ระบบเทคโนโลยีสารสนเทศ (Information Technology System)** หมายถึง ระบบงานขององค์กรที่นำเอาเทคโนโลยีสารสนเทศระบบคอมพิวเตอร์ และระบบเครือข่าย มาช่วยในการสร้างสารสนเทศที่องค์กรสามารถนำมาใช้ประโยชน์ในการวางแผน บริหาร การสนับสนุนการให้บริการ การพัฒนา การควบคุม การติดต่อสื่อสาร ซึ่งมีองค์ประกอบ เช่น ระบบคอมพิวเตอร์ ระบบเครือข่าย แอพพลิเคชั่น ข้อมูล และสารสนเทศ เป็นต้น
18. **เจ้าของข้อมูล** หมายถึง ผู้ได้รับอำนาจจากผู้บังคับบัญชาให้รับผิดชอบข้อมูลของระบบงาน โดยเจ้าของข้อมูลเป็นผู้รับผิดชอบข้อมูลนั้น ๆ หรือได้รับผลกระทบโดยตรงหากข้อมูลเหล่านั้นเกิดสูญหาย
19. **รหัสผ่าน (Password)** หมายถึง ตัวอักษรหรืออักขระหรือตัวเลข ที่ใช้เป็นเครื่องมือในการตรวจสอบยืนยันตัวบุคคลเพื่อควบคุมการเข้าถึงข้อมูลและระบบข้อมูลในการรักษาความมั่นคงปลอดภัยของข้อมูล และระบบเทคโนโลยีสารสนเทศ
20. **ชุดคำสั่งไม่พึงประสงค์ (Malicious software)** หมายถึง ชุดคำสั่งที่มีผลทำให้คอมพิวเตอร์ หรือระบบ คอมพิวเตอร์หรือชุดคำสั่งอื่นเกิดความเสียหาย ถูกทำลาย ถูกแก้ไขเปลี่ยนแปลงหรือเพิ่มเติม ขัดข้องหรือ ปฏิบัติงานไม่ตรงตามคำสั่งที่กำหนดไว้
21. **ระยะเวลาเป้าหมายในการเรียกคืนการดำเนินงาน (Recovery Time Objective : RTO)** หมายถึงระยะเวลาที่กำหนดขึ้นเพื่อเป็นเวลาเป้าหมายในการเรียกคืนการดำเนินงาน
22. **สถานะเป้าหมายในการเรียกคืนการดำเนินงาน (Recovery Point Objective : RPO)** หมายถึง สถานะของการดำเนินงานที่เป็นเป้าหมายในการเรียกคืนการดำเนินงาน หรืออายุของข้อมูลสำรองสำหรับการดำเนินงานที่พร้อมใช้ในการเรียกคืนการดำเนินงาน
23. **ระบบและอุปกรณ์เครือข่าย** หมายถึง ระบบและอุปกรณ์ที่สามารถใช้ในการติดต่อสื่อสารหรือการส่งข้อมูล และสารสนเทศระหว่างระบบเทคโนโลยีสารสนเทศต่าง ๆ ขององค์กร
24. **โครงสร้างพื้นฐานสารสนเทศ** หมายถึง ระบบคอมพิวเตอร์ และระบบเครือข่ายในการสนับสนุนการให้บริการควบคุมการติดต่อสื่อสาร ซึ่งมีองค์ประกอบ เช่น ระบบคอมพิวเตอร์ ระบบเครือข่าย แอพพลิเคชั่น ข้อมูลและสารสนเทศ เป็นต้น
25. **ห้องเซิร์ฟเวอร์ (Server room)** หมายถึง ห้องที่เป็นที่ติดตั้งและเก็บรักษาคอมพิวเตอร์แม่ข่ายของระบบคอมพิวเตอร์และระบบเครือข่ายของคณะ ในการสนับสนุนการให้บริการต่างๆทางด้านเทคโนโลยีสารสนเทศ
26. **ทรัพยากรของระบบ** หมายถึง แหล่งที่มาของระบบสารสนเทศ เช่น ซีพียู หน่วยความจำ พื้นที่ฮาร์ดดิสก์ และปริมาณการใช้เครือข่าย เป็นต้น

27. **ความมั่นคงปลอดภัยด้านการบริหารจัดการ (Administrative Security)** หมายถึง การกระทำในระดับบริหารโดยกำหนดนโยบาย มาตรการ หลักเกณฑ์ หรือกระบวนการ เพื่อนำมาใช้ในการคัดเลือก การพัฒนา การนำไปใช้ หรือการบำรุงรักษาทรัพย์สินสารสนทศให้มีความมั่นคงปลอดภัย
28. **ความมั่นคงปลอดภัยทางด้านกายภาพ (Physical Security)** หมายถึง การจัดให้มีนโยบาย มาตรการหลักเกณฑ์ หรือกระบวนการใด ๆ เพื่อนำมาใช้ในการป้องกันทรัพย์สินสารสนเทศ สิ่งปลูกสร้าง หรือทรัพย์สินอื่นใดจากการคุกคามของบุคคล ภัยธรรมชาติ อุบัติภัย หรือภัยทางกายภาพอื่น

---

# นโยบายการรักษาความมั่นคงปลอดภัยสารสนเทศ

## (1) การจัดโครงสร้างความมั่นคงปลอดภัยข้อมูลสารสนเทศ

## (Organization of information security)

### 1.1 การจัดการความมั่นคงปลอดภัยของหน่วยงานภายในองค์กร

1.1.1 กำหนดผู้มีหน้าที่รับผิดชอบในการบริหารจัดการความมั่นคงปลอดภัยของข้อมูลสารสนเทศ โดยมีการแต่งตั้งคณะกรรมการบริหารจัดการระบบความมั่นคงปลอดภัยข้อมูลสารสนเทศ (ISMS Management Committee) ประกอบด้วยผู้แทนจากหน่วยงานต่างๆภายในองค์กร เพื่อกำกับดูแลในการบริหารจัดการความมั่นคงปลอดภัยข้อมูลสารสนเทศให้เป็นไปในทิศทางเดียวกัน รวมถึงการให้การสนับสนุนทรัพยากรที่จำเป็นในการ พัฒนาระบบบริหารจัดการความมั่นคงปลอดภัยข้อมูลสารสนเทศ

1.1.2 กำหนดบทบาทหน้าที่ของผู้ปฏิบัติงาน หน้าที่ในการบริหารจัดการระบบสารสนเทศ และระบบเครือข่าย ควรต้องแยกออกจากกัน ไม่ควรให้ผู้ปฏิบัติงานคนเดียวกันทำงานที่สำคัญในกระบวนการเดียวกัน เพื่อป้องกันการทุจริตและการสะดุดหยุดชะงักของงานหากผู้ปฏิบัติงานดังกล่าวไม่สามารถมาปฏิบัติงานได้ ยกเว้นแต่มีข้อจำกัดเรื่องจำนวนของผู้ปฏิบัติงาน

1.1.3 การติดต่อกับหน่วยงานที่เกี่ยวข้อง (Contact with Authorities) ให้มีการจัดทำรายชื่อพร้อมหมายเลขโทรศัพท์ ที่อยู่และเว็บไซต์ของหน่วยงานภาครัฐหรือหน่วยงานอื่นๆ ที่เกี่ยวข้อง เพื่อใช้ติดต่อในกรณีฉุกเฉินหรือเกิดเหตุการณ์ละเมิดด้านความมั่นคงปลอดภัยที่ต้องมีการดำเนินการทางกฎหมาย เช่น กระทรวง รัฐวิสาหกิจ สถานีตำรวจ สถานีดับเพลิง ผู้ให้บริการเชื่อมต่ออินเทอร์เน็ต เป็นต้น โดยต้องมีการทบทวนข้อมูลดังกล่าวให้ถูกต้องและเป็นปัจจุบันเสมอ

1.1.4 การติดต่อกลุ่มผู้เชี่ยวชาญที่เกี่ยวข้องด้านความมั่นคงปลอดภัยโดยสมัครเป็นสมาชิกในการรับข่าวสารด้านความมั่นคงปลอดภัย จากหน่วยงานหรือเว็บไซต์ของเจ้าของผลิตภัณฑ์ เพื่อใช้เป็นประโยชน์ในการดำเนินการดังนี้

- รับทราบข่าวสารด้านความมั่นคงปลอดภัย
- เพื่อแลกเปลี่ยนแนวทางการดำเนินการด้านความมั่นคงปลอดภัย
- เพื่ออัพเดทเทคโนโลยีที่ใช้ในการบริหารจัดการความมั่นคงปลอดภัย

1.1.5 ในการบริหารจัดการโครงการเพื่อจัดหาระบบสารสนเทศใดๆ จะต้องได้รับความเห็นชอบจากผู้บริหารขององค์กร โดยต้องทำการทบทวนความสอดคล้องกับนโยบายการรักษาความมั่นคงปลอดภัยสารสนเทศขององค์กร

ผลกระทบต่อระบบสารสนเทศ ความต้องการใช้งานและความเข้ากันได้เชิงเทคโนโลยี โดยผลการอนุมัติดังกล่าวจะต้องมีการจัดทำเป็นลายลักษณ์อักษร

## 1.2 การควบคุมการใช้งานอุปกรณ์แบบพกพาและการปฏิบัติงานจากระยะไกล (Mobile device and teleworking)

1.2.1 การใช้คอมพิวเตอร์แบบพกพา

1.2.1.1 เครื่องคอมพิวเตอร์แบบพกพาที่องค์กรจัดหาให้ใช้เป็นทรัพย์สินขององค์กร ซึ่งต้องมีหมายเลขทะเบียนครุภัณฑ์ควบคุมที่ออกโดยงานคลังและพัสดุ

1.2.1.2 ซอฟต์แวร์ที่ได้ติดตั้งบนเครื่องคอมพิวเตอร์แบบพกพาของหน่วยงาน ต้องเป็นซอฟต์แวร์ที่มีลิขสิทธิ์ถูกต้องตามกฎหมาย

1.2.1.3 ห้ามผู้ใช้งานคัดลอกโปรแกรมต่างๆ ที่ได้ถูกติดตั้งลงบนเครื่องคอมพิวเตอร์แบบพกพาของหน่วยงานซึ่งมีลิขสิทธิ์ถูกต้องตามกฎหมาย นำไปติดตั้งบนเครื่องคอมพิวเตอร์ส่วนตัว หรือแก้ไขหรือนำไปให้ผู้อื่นใช้งานโดยผิดกฎหมาย

1.2.1.4 ไม่ดัดแปลงแก้ไขส่วนประกอบต่างๆ ของคอมพิวเตอร์พกพา ต้องรักษาสภาพของคอมพิวเตอร์พกพาให้มีสภาพเดิม

1.2.1.5 การควบคุมการใช้งานระบบสารสนเทศ

1) คอมพิวเตอร์แบบพกพาขององค์กรที่ต้องการนำไปใช้นอกสถานที่ในกิจกรรมขององค์กรจะต้องได้รับการอนุมัติจากหัวหน้างานเทคโนโลยีทางการศึกษา โดยอุปกรณ์ดังกล่าวจะต้องมีการควบคุมด้านความมั่นคงปลอดภัยในระดับเดียวกับอุปกรณ์ที่ใช้ในสำนักงาน
2) คอมพิวเตอร์แบบพกพาก่อนที่จะเชื่อมต่อเข้ากับระบบเครือข่ายของหน่วยงาน ควรอัพเดท Antivirus และ Virus Definition ให้เป็นปัจจุบันอยู่เสมอ
3) ต้องกำหนดชื่อผู้ใช้งาน (Username) และรหัสผ่าน (Password) ในการเข้าใช้งาน โดยกำหนดให้มีตัวอักษรมากกว่าหรือเท่ากับ 8 ตัวอักษร โดยมีการผสมระหว่างตัวอักษร ตัวเลข และสัญลักษณ์เข้าด้วยกัน
4) ตั้งการใช้งานโปรแกรมรักษาจอภาพ (Screen Saver) โดยตั้งเวลาประมาณ 10 นาที ให้ทำการล็อคหน้าจอเมื่อไม่มีการใช้งาน หลังจากนั้นเมื่อต้องการใช้งานต้องใส่รหัสผ่าน
5) ต้องออกจากระบบ (Log out) ทันทีเมื่อเลิกใช้งานหรือไม่อยู่ที่หน้าจอเป็นเวลานาน
6) ข้อมูลสารสนเทศขององค์กรที่อยู่ในเครื่องคอมพิวเตอร์แบบพกพาจะต้องทำการสำรองข้อมูลลงบนสื่อบันทึกข้อมูลไว้อย่างสม่ำเสมอ เพื่อป้องกันการสูญหายของข้อมูล

7) เก็บรักษาสื่อสำรองข้อมูล (Backup Media) ไว้ในสถานที่ที่เหมาะสมไม่เสี่ยงต่อการรั่วไหลของข้อมูล

8) สื่อสำรองข้อมูลที่ไม่ใช้งานแล้ว ต้องทำลายไม่ให้สามารถนำไปใช้งานได้อีก โดยการทำลายสื่อบันทึกที่หมดอายุการใช้งานหรือชำรุด ให้ปฏิบัติตามระเบียบปฏิบัติเรื่อง การทำลายข้อมูลและสื่อบันทึกข้อมูล (รหัสเอกสาร PM-MS-07: Disposal of Media Procedure)

1.2.1.6 การป้องกันทางกายภาพ (Physical)

1) การเคลื่อนย้ายควรใส่กระเป๋าสำหรับเครื่องคอมพิวเตอร์แบบพกพา เพื่อป้องกันอันตรายที่เกิดจากการกระทบกระเทือน เช่น การตกจากโต๊ะทำงาน หรือพลัดหลุดมือ หลีกเลี่ยงการใส่เครื่องคอมพิวเตอร์พกพาไว้ในกระเป๋าเดินทาง เพราะอาจถูกกดทับ เกิดความเสียหายได้

2) การเคลื่อนย้ายเครื่องขณะที่เครื่องเปิดใช้งานอยู่ ให้ทำการยกจากฐานภายใต้แป้นพิมพ์ ห้ามย้ายเครื่องโดยการดึงหน้าจอภาพขึ้น

3) ผู้ใช้งานมีหน้าที่รับผิดชอบในการป้องกันการสูญหาย เช่น เก็บรักษาไว้ในสถานที่ที่ปลอดภัย ไม่วางเครื่องทิ้งไว้ในที่สาธารณะ หรือในบริเวณที่มีความเสี่ยงต่อการสูญหาย

4) ไม่เก็บหรือใช้งานคอมพิวเตอร์แบบพกพาในสถานที่ที่มีความร้อน/ความชื้น/ฝุ่นละอองสูง และต้องระวังป้องกันการตกหล่น

5) หลีกเลี่ยงการวางเครื่องคอมพิวเตอร์พกพาไว้ใกล้อุปกรณ์ที่มีสนามแม่เหล็กไฟฟ้าแรงสูงในระยะใกล้ เช่น โทรทัศน์ ไมโครเวฟ ตู้เย็น เป็นต้น และวางไว้หรือใช้งานในที่ที่มีแรงสั่นสะเทือนมาก เช่น ยานพาหนะที่กำลังเคลื่อนที่

6) หลีกเลี่ยงการใช้วัสดุ หรือของแข็ง เช่น ปลายปากกา กดสัมผัสหน้าจอ LCD ให้เป็นรอยขีดข่วน ไม่วางของทับบนเครื่อง ซึ่งอาจทำให้จอ LCD ของเครื่อง แตกเสียหายได้

7) การเช็ดทำความสะอาดหน้าจอภาพต้องเช็ดด้วยความระมัดระวัง ควรเช็ดไปในทางเดียวกัน ไม่ควรเช็ดแบบหมุนวน เพราะจะทำให้หน้าจอมีรอยขีดข่วนได้

1.2.2 การปฏิบัติงานจากระยะไกล (Teleworking)

1.2.2.1 การเข้าสู่ระบบจากระยะไกล (Remote access) สู่ระบบเครือข่ายคอมพิวเตอร์ขององค์กร ก่อให้เกิดช่องทางที่มีความเสี่ยงสูงต่อความปลอดภัยของข้อมูลและทรัพยากรขององค์กร การควบคุมบุคคลที่เข้าสู่ระบบขององค์กรจากระยะไกลต้องเชื่อมต่อผ่านระบบ Virtual Private Network (VPN) เท่านั้น

1.2.2.2 วิธีการใดๆก็ตามที่สามารถเข้าสู่ข้อมูลหรือระบบข้อมูลได้จากระยะไกลต้องจัดทำหนังสือเป็นลายลักษณ์อักษรและได้รับการอนุมัติจากผู้บังคับบัญชาตามลำดับชั้นหรือผู้ที่ได้รับการมอบอำนาจ โดยระบุรายละเอียดดังนี้

1) เหตุผลความจำเป็นที่ต้องปฏิบัติงานจากภายนอกหน่วยงาน

2) รายละเอียดและลักษณะของระบบงาน

3) ช่องทางที่ใช้ในการปฏิบัติงานจากภายนอก

4) รายชื่อผู้ใช้งานหรือกลุ่มผู้ใช้งาน

5) ช่วงเวลาและระยะเวลาในการปฏิบัติงานจากภายนอกหน่วยงาน

1.2.2.3 ไม่อนุญาตให้ปฏิบัติงานจากภายนอกหน่วยงานสำหรับระบบงานที่มีความลับในระดับชั้นลับและชั้นลับมาก ตามข้อกำหนดในระเบียบปฏิบัติ เรื่อง การจัดระดับชั้นของข้อมูล (รหัสเอกสาร PM-MS-06)

1.2.2.4 การเข้าสู่ระบบสารสนเทศขององค์กรจากระยะไกลต้องมีการลงบันทึกเข้าใช้งาน (Login) โดยแสดงตัวตนด้วยชื่อผู้ใช้งาน และมีการพิสูจน์ยืนยันตัวตน (Authentication) ด้วยการใช้รหัสผ่าน เพื่อตรวจสอบความถูกต้องของผู้ใช้งานก่อนทุกครั้ง

1.2.2.5 การอนุญาตให้ผู้ใช้งานเข้าสู่ระบบจากระยะไกลต้องอยู่บนพื้นฐานของความจำเป็นเท่านั้น และไม่เปิดช่องทางติดต่อ (Port) และอุปกรณ์เชื่อมต่อระยะไกล ยกเว้นเฉพาะที่ได้รับอนุญาตเท่านั้น

---

# นโยบายการรักษาความมั่นคงปลอดภัยสารสนเทศ

## (2) การบริหารจัดการทรัพย์สิน

## (Asset management)

### 2.1 ความรับผิดชอบต่อทรัพย์สิน

2.1.1 การจัดทำบัญชีรายการทรัพย์สิน

2.1.1.1 ต้องจัดทำบัญชีทรัพย์สินทั้งหมดที่เกี่ยวข้องกับการดำเนินงานและการให้บริการในขอบเขตของการขอรับการรับรองมาตรฐานการรักษาความปลอดภัยสารสนเทศ โดยให้ครอบคลุมทรัพย์สินประเภทต่างๆ ดังต่อไปนี้

- กระบวนการ (Business process)
- ข้อมูลสารสนเทศ (Information)
- ฮาร์ดแวร์ (Hardware)
- ซอฟต์แวร์ (Software)
- บุคลากร (Personnel)
- บริการจากภายนอก (Outsource service)

2.1.1.2 ต้องมีการทบทวนบัญชีทรัพย์สินอย่างน้อย ปีละ 1 ครั้ง เพื่อตรวจสอบความถูกต้องครบถ้วนของบัญชีรายการทรัพย์สินของหน่วยงาน

2.1.2 กำหนดผู้รับผิดชอบ หรือผู้ถือครองทรัพย์สิน (Ownership of Assets)

2.1.2.1 ทรัพย์สินทั้งหมดจะต้องกำหนดให้มีผู้รับผิดชอบ หรือผู้ถือครองอย่างชัดเจน โดยผู้ถือครองทรัพย์สินดังกล่าว อาจระบุเป็นชื่อบุคคลหรือชื่อหน่วยงานได้ กรณีที่ทรัพย์สินใดเป็นของหน่วยงาน ความรับผิดชอบต่อทรัพย์สินดังกล่าวจะเป็นของหัวหน้าหน่วยงานนั้น

2.1.2.2 ผู้ถือครองทรัพย์สินสามารถกำหนดผู้ที่จะสามารถใช้งานหรือเข้าถึงทรัพย์สินของตนได้

2.1.2.3 ผู้ถือครองทรัพย์สินจะต้องพิจารณากำหนดระดับชั้นความลับของข้อมูลในทรัพย์สินที่ตนเองเป็นเจ้าของหรือถือครองอยู่ ตรวจสอบการใช้งานทรัพย์สินของตนเองให้เป็นไปตามข้อกำหนดในการจัดการระดับชั้นความลับของข้อมูลและสารสนเทศ รวมทั้งทบทวนความเหมาะสมของระดับชั้นความลับที่กำหนดไว้อย่างสม่ำเสมอ

2.1.3 การใช้งานทรัพย์สินอย่างเหมาะสม (Acceptable use of assets)

2.1.3.1 ระบบสารสนเทศใดๆ ขององค์กร จะต้องนำไปใช้เพื่อวัตถุประสงค์ขององค์กรเท่านั้นโดย

1) การใช้งานระบบสารสนเทศจะจำกัดให้เฉพาะผู้ใช้งานที่ได้รับอนุญาตจากองค์กรเท่านั้น ไม่ครอบคลุมไปถึงบุคคลในครอบครัวหรือบุคคลอื่น ๆ
2) การใช้งานต้องไม่ก่อให้เกิดค่าใช้จ่ายโดยตรงต่อองค์กร
3) การใช้งานจะต้องไม่เป็นการขัดขวางประสิทธิภาพในการปฏิบัติงานภายในองค์กร
4) จะต้องไม่มีการส่งหรือรับไฟล์หรือเอกสารใดๆซึ่งอาจก่อให้เกิดผลกระทบทางกฎหมายหรือมีผลกระทบต่อภาพลักษณ์ขององค์กร
5) ข้อมูล ข้อความ ไฟล์ และเอกสารใด ๆ ที่จัดเก็บไว้ในระบบสารสนเทศขององค์กร ให้ถือเป็นทรัพย์สินขององค์กร

**2.2 การแบ่งระดับชั้นของข้อมูลสารสนเทศ**

2.2.1 มีข้อกำหนดในการแบ่งระดับชั้นความลับของข้อมูลและสารสนเทศอย่างชัดเจนข้อมูลทั้งหมดจะต้องได้รับการแบ่งประเภทตามมาตรฐานการจัดระดับชั้นความลับของข้อมูลและสารสนเทศ

2.2.2 การจัดทำข้อความระบุชั้นความลับและการจัดการข้อมูลจะต้องได้รับ การจัดทำ จัดเก็บ นำส่ง ประมวลผล ทำลาย โดยให้เป็นไปตามระเบียบปฏิบัติ เรื่อง การจัดระดับชั้นของข้อมูลสารสนเทศ (รหัสเอกสาร PM-MS-06 : Information Classification Procedure) ผู้ที่เป็นเจ้าของข้อมูลจะต้องจัดทำป้ายข้อความระบุชั้นความลับของข้อมูลให้ชัดเจน หากจำเป็นต้องมีการส่งข้อมูลไปให้บุคคลภายนอก ผู้ที่รับผิดชอบในการส่งข้อมูลดังกล่าวจะต้องแจ้งให้ผู้รับทราบถึงระดับชั้นความลับของข้อมูลดังกล่าว ตลอดจนข้อกำหนดในการจัดการกับข้อมูลก่อนนำส่ง

**2.3 การจัดการสื่อบันทึกข้อมูล (Media handling)**

2.3.1 สื่อบันทึกข้อมูลที่แยกถอดได้จะต้องได้รับการจัดการตามระดับชั้นความลับสูงสุดของข้อมูลที่อยู่ในสื่อบันทึกข้อมูลนั้น

2.3.2 การกำจัดสื่อบันทึกข้อมูล สื่อบันทึกข้อมูลที่ไม่ต้องการให้สามารถนำกลับมาใช้ได้อีก จะต้องถูกทำลายตามข้อกำหนดที่ระบุไว้ในระเบียบปฏิบัติ เรื่อง การทำลายข้อมูลและสื่อบันทึกข้อมูล (รหัสเอกสาร PM-MS-07: Disposal of Media Procedure)

2.3.3 การนำส่งสื่อบันทึกข้อมูลออกไปภายนอกองค์กร (Physical media transfer) สื่อบันทึกข้อมูลที่นำออกไปใช้ภายนอกองค์กร ต้องได้รับการป้องกันอย่างเหมาะสม ผู้นำส่งสื่อบันทึกข้อมูล ต้องเป็น บุคคลหรือหน่วยงานที่ได้รับการรับรองและเชื่อถือได้

---

# นโยบายการรักษาความมั่นคงปลอดภัยสารสนเทศ

## (3) การควบคุมการเข้าถึง

## (Access control)

### 3.1 การควบคุมการเข้าถึงระบบสารสนเทศตามภารกิจ

3.1.1 การจัดการสิทธิ์การเข้าถึง

1) เจ้าของระบบสารสนเทศจะต้องกำหนดสิทธิ์ในการเข้าถึงตามภาระหน้าที่และความจำเป็นในการปฏิบัติงาน มีบันทึกรายละเอียดการกำหนดสิทธิ์การเข้าถึงระบบสารสนเทศและการแก้ไขเปลี่ยนแปลงสิทธิ์ต่างๆเพื่อเป็นหลักฐานในการตรวจสอบภายหลัง
2) ให้มีการติดตั้งระบบบันทึกและติดตามการใช้งานระบบสารสนเทศขององค์กร และการเฝ้าระวังการใช้งาน ไม่ให้ผู้ใช้งานล่วงละเมิดความปลอดภัย และล่วงละเมิดสิทธิ์ของผู้ใช้งานอื่นด้วย
3) ให้มีการทบทวนสิทธิ์ของผู้ใช้งานแต่ละคนอย่างน้อยปีละ 1 ครั้ง เพื่อให้เหมาะสมต่อภาระหน้าที่และการปฏิบัติงาน ตลอดจนเพื่อป้องกันผลกระทบต่อมาตรการความมั่นคงปลอดภัยของระบบสารสนเทศในองค์กร

3.1.2 การควบคุมการเข้าใช้งานระบบเครือข่าย

1) การขอใช้งานระบบเครือข่าย ต้องให้ผู้ที่มีความประสงค์แจ้งขออนุมัติต่อหัวหน้างานเทคโนโลยีทางการศึกษาเป็นลายลักษณ์อักษร
2) การเชื่อมต่อเครื่องคอมพิวเตอร์เพื่อเข้าใช้งานอินเตอร์เน็ต ต้องเชื่อมต่อผ่านระบบเครือข่ายที่องค์กรจัดไว้ให้เท่านั้น

### 3.2 การบริหารจัดการการเข้าถึงของผู้ใช้งาน

3.2.1 การเปิดสิทธิ์และการเพิกถอนสิทธิ์ผู้ใช้งานให้ปฏิบัติตามขั้นตอนที่ระบุไว้ในระเบียบปฏิบัติ เรื่อง การบริหารจัดการสิทธิ์ผู้ใช้งาน (รหัสเอกสาร PM-SW-01: User access management procedure)

3.2.2 ผู้ใช้งานแต่ละคนต้องมี User Account ที่ไม่ซ้ำกัน ไม่อนุญาตให้ใช้ User account ร่วมกัน การใช้ User Account แบบกลุ่ม อนุญาตให้เฉพาะกับบางระบบที่จำเป็นเท่านั้น

3.2.3 การขอใช้งานระบบงานใด ๆ จะต้องได้รับการอนุมัติอย่างเป็นทางการจากผู้บริหารหรือเจ้าของระบบ

3.2.4 กรณีที่ต้องให้สิทธิ์พิเศษนอกเหนือจากภาระงานที่กำหนด จะต้องได้รับการอนุมัติเห็นชอบจากหัวหน้าหน่วยงานเจ้าของระบบ จัดทำคำร้องเป็นลายลักษณ์อักษร โดยการให้สิทธิ์พิเศษดังกล่าวจะต้องกำหนดช่วงเวลาที่ชัดเจน และเมื่อพ้นกำหนดการให้สิทธิ์พิเศษจะต้องระงับการใช้งานทันที

### 3.3 หน้าที่ความรับผิดชอบของผู้ใช้งาน

3.3.1 ผู้ใช้งานจะต้องไม่เปิดเผย User Account และรหัสผ่านต่อผู้อื่น และต้องไม่อนุญาตให้ผู้อื่นใช้ User Account และรหัสผ่าน (Password) ของตนในการเข้าใช้งานเครื่องคอมพิวเตอร์ของหน่วยงานร่วมกัน

3.3.2 การใช้รหัสผ่าน

3.3.2.1 รหัสผ่านต้องมีอย่างน้อย 8 ตัวอักษร ยกเว้นกรณีที่มีข้อจำกัดทางเทคนิค

3.3.2.2 รหัสผ่านต้องประกอบด้วยอักษรตัวใหญ่ อักษรตัวเล็ก ตัวเลขและอักขระพิเศษ (เช่น $,!(*)/ และช่องว่าง) ผสมกัน

3.3.2.3 รหัสผ่านไม่ควรจะให้ผู้อื่นคาดเดาได้ง่ายหรือคาดเดาได้จากคำต่าง ๆ ที่พบในพจนานุกรม ชื่อบริษัท ตำแหน่งทางภูมิศาสตร์ ตัวละครในนิยายที่รู้จักกันทั่วไปจากหนังสือหรือภาพยนตร์ เป็นต้น

3.3.2.4 รหัสผ่านไม่ควรตั้งจากข้อมูลส่วนตัวของผู้ใช้งาน

3.3.2.5 เปลี่ยนรหัสผ่านเมื่อพบว่า มีผู้อื่นนำรหัสผ่านไปใช้งาน

3.3.2.6 ผู้ใช้งานต้องเปลี่ยนรหัสผ่านเริ่มต้นทันทีหลังจากสามารถเข้าใช้งานระบบได้ในครั้งแรก

3.3.2.7 ผู้ใช้งานทั่วไปต้องเปลี่ยนรหัสผ่านทุก 180 วัน และผู้ดูแลระบบหรือผู้มีสิทธิ์พิเศษต้องเปลี่ยนรหัสผ่านทุก 1 ปี หรือทุกครั้งที่มีการแจ้งเตือน โดยการเปลี่ยนรหัสผ่าน ต้องไม่ซ้ำกับรหัสที่ได้ใช้ไปครั้งล่าสุด

3.3.2.8 ไม่ใช้โปรแกรมคอมพิวเตอร์ช่วยในการจำรหัสผ่านส่วนบุคคลอัตโนมัติ (Save password) สำหรับเครื่องคอมพิวเตอร์ส่วนบุคคลที่ผู้ใช้งานครอบครองอยู่

3.3.2.9 ไม่จดหรือบันทึกรหัสผ่านส่วนบุคคลไว้ในสถานที่ที่ง่ายต่อการสังเกตเห็นของบุคคลอื่น

### 3.4 การควบคุมการเข้าถึงระบบและแอพพลิเคชั่น

3.4.1 การจำกัดการเข้าถึงระบบสารสนเทศ

3.4.1.1 ผู้ดูแลระบบต้องกำหนดการลงทะเบียนผู้ใช้งานของหน่วยงานตามขั้นตอนที่ระบุไว้ในระเบียบปฏิบัติ เรื่อง การบริหารจัดการสิทธิ์ผู้ใช้งาน (รหัสเอกสาร PM-SW-01: User access management procedure) เพื่อควบคุมและจำกัดสิทธิการเข้าถึงระบบสารสนเทศและข้อมูล

3.4.1.2 จำกัดระยะเวลาการเชื่อมต่อระบบสารสนเทศต่างๆ และหากไม่มีการใช้งานนานเกินระยะเวลา 30 นาที ต้องยกเลิกการเชื่อมต่อระบบเมื่อครบกำหนดเวลา

3.4.1.3 ระบบซึ่งไวต่อการรบกวน มีผลกระทบและมีความสำคัญสูงต่อองค์กร หรือหน่วยงานต้องแยกออกจากระบบอื่นๆ และมีการควบคุมสภาพแวดล้อมโดยเฉพาะ

3.4.2 การเข้าใช้งานที่มั่นคงปลอดภัย

3.4.2.1 กำหนดให้ระบบไม่แสดงรายละเอียดสำคัญหรือความผิดพลาดต่างๆ ของระบบก่อนที่การเข้าสู่ระบบจะเสร็จสมบูรณ์

3.4.2.2 กำหนดให้ผู้ใช้งานใส่รหัสผ่านผิดพลาดได้ไม่เกิน 3 ครั้ง หากเกิน 3 ครั้ง ระบบจะถูกล็อคเป็นระยะเวลาอย่างน้อย 1 ชั่วโมง

3.4.3 การบริหารจัดการรหัสผ่าน (Password Management System)

3.4.3.1 กำหนดให้มีระบบบริหารจัดการรหัสผ่านที่สามารถทำงานเชิงโต้ตอบ (Interactive) หรือมีการทำงานในลักษณะอัตโนมัติซึ่งเอื้อต่อการกำหนดรหัสผ่านที่มีคุณภาพ โดยปฏิบัติตามระเบียบปฏิบัติ เรื่อง การบริหารรหัสผ่านของผู้ใช้งาน (รหัสเอกสาร PM-SW-02: User password management procedure)

3.4.4 การใช้งานโปรแกรมอรรถประโยชน์ (Use of System Utilities) การลงโปรแกรมอรรถประโยชน์เพื่อการใช้งานบนคอมพิวเตอร์ของหน่วยงาน ต้องเป็นโปรแกรมที่มีลิขสิทธิ์ถูกต้องเท่านั้น

3.4.5 การควบคุมการเข้าถึงซอร์สโค้ดของโปรแกรม

3.4.5.1 กำหนดให้มีการจัดเก็บซอร์สโค้ดและไลบรารีสำหรับซอฟต์แวร์ของระบบสารสนเทศไว้ในสถานที่ที่มีความมั่นคงปลอดภัย มีการควบคุมเวอร์ชั่น และจำกัดสิทธิ์การเข้าถึงได้เฉพาะผู้ได้รับอนุญาตเท่านั้น

3.4.5.2 จัดเก็บซอฟต์แวร์เวอร์ชั่นเก่า ข้อมูลที่เกี่ยวข้องกับระบบสารสนเทศเดิม ที่ไม่ได้ใช้งานไว้อย่างปลอดภัยเพื่อใช้อ้างอิง

---

# นโยบายการรักษาความมั่นคงปลอดภัยสารสนเทศ

## (4) การเข้ารหัสข้อมูล (Cryptography)

**4.1 มาตรการการเข้ารหัสข้อมูล**

4.1.1 ควรใช้การเข้ารหัสสำหรับการเชื่อมต่อเครือข่ายทั้งหมด เช่น https, ssh เป็นต้น

4.1.2 การกำหนดมาตรการรักษาความมั่นคงปลอดภัยของข้อมูล โดยใช้มาตรฐานการรักษาความปลอดภัยของข้อมูลด้วยเทคโนโลยี Secured Socket Layer (SSL) ซึ่งผู้ใช้บริการสามารถสังเกตได้จากชื่อของ URL (Uniform Resource Locator) ที่เป็น https://

4.1.3 ข้อมูลทั้งหมดที่ถูกส่งผ่านเครือข่ายอินเทอร์เน็ตจะถูกเข้ารหัสตามมาตรฐาน IEEE 802.xx จึงมีการรักษาการเป็นความลับ (Confidentiality) สามารถยืนยันความถูกต้องได้ (Integrity) และหากข้อมูลถูกขโมยไประหว่างการส่งผ่านระบบเครือข่าย ข้อมูลจะไม่สามารถนำไปใช้ได้เนื่องจากถูกเข้ารหัสอยู่

4.1.4 ควรมีการ hashing รหัสผ่านสำหรับการเข้าใช้งานระบบด้วยวิธีการเข้ารหัสต่าง ๆ เช่น SHA-1, SHA-2, MD5 เป็นต้น เพื่อเพิ่มความปลอดภัยของรหัสผ่านของผู้ใช้บริการและการรักษาเป็นความลับ

---

# นโยบายการรักษาความมั่นคงปลอดภัยสารสนเทศ

## (5) ความมั่นคงปลอดภัยทางกายภาพและสิ่งแวดล้อม

## (Physical and environmental security)

### 5.1 พื้นที่ที่ต้องมีการรักษาความมั่นคงปลอดภัย (Secure Area)

5.1.1 ขอบเขตการรักษาความปลอดภัยทางกายภาพ (Physical Security Perimeter) ต้องกำหนดพื้นที่ที่ต้องมีการรักษาความมั่นคงปลอดภัยให้ชัดเจน มีการควบคุมการเข้าออกพื้นที่อย่างเข้มงวด เพื่อป้องกันการบุกรุกจากภายนอก รวมทั้งดูแลจัดเก็บอุปกรณ์ระบบสารสนเทศภายในพื้นที่อย่างเหมาะสม

5.1.2 การควบคุมการเข้าออกทางกายภาพ ให้หัวหน้าหน่วยงานเทคโนโลยีทางการศึกษามีอำนาจในการกำหนดสิทธิ์การเข้าออกพื้นที่ โดยพิจารณาจากความจำเป็นในการเข้ามาในพื้นที่ดังกล่าว ในการเข้าออกพื้นที่ควบคุมนอกเหนือจากสิทธิ์ที่กำหนดไว้แล้วนั้น จะต้องได้รับการอนุมัติจากเจ้าของพื้นที่หรือผู้ได้รับมอบหมายเป็นลายลักษณ์อักษรก่อนทุกครั้ง ผู้ที่เข้ามาในพื้นที่ที่มีการรักษาความมั่นคงปลอดภัย จะต้องปฏิบัติตามกระบวนการควบคุมการเข้าออกพื้นที่ที่เจ้าของพื้นที่กำหนด

5.1.3 การรักษาความปลอดภัยของสำนักงาน และพื้นที่เกี่ยวข้องกับการปฏิบัติงานที่มีความสำคัญ เช่น ห้อง Server ไม่อนุญาตให้เข้าหากไม่ได้รับอนุญาตจากหัวหน้าหน่วยงานและต้องมีการควบคุมการผ่านเข้าออกอย่างเข้มงวด ในช่วงเวลาที่ไม่มีผู้ดูแลจะต้องห้ามผ่านเข้าออกห้องทำงานหรือห้องที่มีระบบสารสนเทศ โดยจะต้องล็อกประตูและหน้าต่างทุกครั้ง

5.1.4 การป้องกันภัยคุกคามจากสิ่งแวดล้อมภายนอก ห้อง Server จะมีการควบคุมการเข้าออกอย่างเข้มงวดและตั้งอยู่ในพื้นที่ที่ปลอดภัยจากภัยทางธรรมชาติ เช่น ดินถล่ม หรือน้ำท่วม เป็นต้น จะต้องมีเครื่องตรวจจับควัน (smoke detector) และมีอุปกรณ์ดับเพลิงอย่างเพียงพอและเหมาะสม นอกจากนี้ต้องดูแลรักษาความสะอาดของพื้นที่โดยทั่วไปอย่างสม่ำเสมอ เพื่อไม่ให้มีวัสดุที่เป็นเชื้อเพลิงอยู่ในพื้นที่ดังกล่าว

5.1.5 การทำงานในพื้นที่หวงห้ามไม่อนุญาตให้นำอุปกรณ์ถ่ายภาพ วิดีโอ หรืออุปกรณ์บันทึกอื่น ๆ เข้ามาภายในบริเวณดังกล่าว เว้นแต่จะได้รับอนุญาต

5.1.6 พื้นที่รับส่งของ (Loading Area) ผู้นำส่งสิ่งของหรืออุปกรณ์ระบบสารสนเทศต่างๆ จะต้องได้รับการอนุญาตให้เข้ามาในพื้นที่ดังกล่าวก่อน จึงจะสามารถเข้ามาในพื้นที่ได้ สิ่งของหรืออุปกรณ์ที่นำเข้ามาจะต้องผ่านการตรวจสอบว่าไม่มีอันตรายก่อนจึงจะทำการเคลื่อนย้ายเข้าในห้อง Server ได้

**5.2 ความปลอดภัยของอุปกรณ์**

5.2.1 การติดตั้งและการป้องกันอุปกรณ์ควรใช้ชั้นวางอุปกรณ์ (Rack) สำหรับวาง server และอุปกรณ์เครือข่ายที่สำคัญอื่นๆ

5.2.2 ระบบสาธารณูปโภคที่ใช้สนับสนุนการปฏิบัติงาน ใช้เครื่องสำรองไฟฟ้าต่อเนื่อง (UPS) เพื่อป้องกันอุปกรณ์จากเหตุการณ์ไฟฟ้าดับหรือไฟฟ้าผิดปกติ ใช้ระบบปรับอากาศเพื่อสร้างสภาพแวดล้อมที่เหมาะสมให้กับการทำงานของระบบสารสนเทศและอุปกรณ์ต่างๆ

5.2.3 การวางสายเคเบิลให้มีความปลอดภัย ต้องมีการป้องกันสายเคเบิลที่มีข้อมูลวิ่งผ่านทั้งหมด เพื่อไม่ให้มีการดักจับข้อมูลหรือสร้างความเสียหายต่อสายเคเบิล ต้องแยกสายไฟทั้งหมดออกจากสายเคเบิลสำหรับระบบสารสนเทศเพื่อป้องกันสัญญาณรบกวน ยกเว้นแต่มีเหตุจำเป็น ต้องจัดหาตู้ชุมสาย หรือตู้ Rack ที่จัดเก็บสายเคเบิลของระบบเครือข่ายให้เหมาะสมและต้องมีการควบคุมการเข้าถึงอุปกรณ์สำคัญเหล่านี้

5.2.4 การบำรุงรักษาอุปกรณ์ ทุกครั้งที่ต้องมีการบำรุงรักษาซ่อมแซมอุปกรณ์ใด ๆ จะต้องทำการบันทึกรายการซ่อมบำรุงรักษาอุปกรณ์ดังกล่าวทุกครั้ง ควรบำรุงรักษาระบบควบคุมสภาพแวดล้อมและอุปกรณ์ต่างๆ ตามคำแนะนำที่ผู้ผลิตระบุไว้ รวมทั้งในระหว่างปิดระบบเพื่อบำรุงรักษาตามแผนกำหนดให้บุคลากรที่ผ่านการฝึกอบรม และได้รับอนุญาตเท่านั้นที่จะสามารถทำการซ่อมบำรุงระบบและอุปกรณ์ต่างๆ ในกรณีที่ใช้บริการซ่อมบำรุงจากผู้ให้บริการจากภายนอก จะต้องกำหนดเงื่อนไขในการบำรุงรักษาให้ชัดเจน

5.2.5 การเคลื่อนย้ายทรัพย์สินสารสนเทศออกไปใช้นอกสถานที่ จะต้องได้รับการอนุญาตจากเจ้าของทรัพย์สินก่อนทุกครั้ง จัดทำบันทึกการนำอุปกรณ์ออกนอกสถานที่และส่งคืน มีการติดตามทรัพย์สินดังกล่าวกลับมาตามช่วงเวลาที่กำหนด และตรวจสอบอุปกรณ์ที่ส่งคืนอยู่ในสภาพดี

5.2.6 การรักษาความปลอดภัยของอุปกรณ์และทรัพย์สินที่ใช้งานนอกสถานที่ทำงาน ผู้ที่รับผิดชอบต้องดูแลป้องกันการสูญหาย เสียหายระหว่างการขนย้าย การเกิดอุบัติเหตุกับอุปกรณ์หรือทรัพย์สินดังกล่าว

5.2.7 การทำลายอุปกรณ์ระบบสารสนเทศหรือการนำกลับมาใช้อีกครั้ง

5.2.7.1 หัวหน้างานเทคโนโลยีทางการศึกษา เป็นผู้อนุมัติการทำลาย หรือนำอุปกรณ์สารสนเทศกลับมาใช้อีกครั้ง โดยผู้ที่ต้องการทำลายหรือนำอุปกรณ์สารสนเทศกลับมาใช้ต้องยื่นเอกสารเป็นลายลักษณ์อักษร

5.2.7.2 ในการทำลายอุปกรณ์ระบบสารสนเทศ ผู้รับผิดชอบต้องปฏิบัติตามขั้นตอนในระเบียบปฏิบัติเรื่องการทำลายข้อมูลและสื่อบันทึกข้อมูล (รหัสเอกสาร PM-MS-07) เพื่อให้มั่นใจได้ว่าข้อมูลใด ๆ ที่อยู่ในอุปกรณ์ดังกล่าวได้ถูกลบทิ้งไปแล้ว โดยที่ไม่สามารถกู้คืนกลับมาใช้ได้อีก

5.2.8 ความปลอดภัยของอุปกรณ์ที่ไม่มีผู้ดูแล เมื่อไม่ต้องการใช้งานอุปกรณ์หรือเครื่องคอมพิวเตอร์แล้ว ให้ทำการยกเลิกการเชื่อมต่อกับระบบเครือข่าย หรือระบบสารสนเทศ จัดเก็บอุปกรณ์หรือเครื่องคอมพิวเตอร์ไว้ในตู้ที่สามารถปิดล็อคได้ เพื่อป้องกันไม่ให้บุคคลอื่นเข้ามาใช้อุปกรณ์ดังกล่าวโดยไม่ได้รับอนุญาต

5.2.9 การเคลียร์หน้าจอคอมพิวเตอร์และการจัดเก็บโต๊ะทำงาน เครื่องคอมพิวเตอร์ทุกเครื่อง ต้องมีการตั้งค่า Screen Saver ที่มีรหัสผ่านป้องกัน หรือการควบคุมอื่นๆ โดยให้เริ่มทำงานหลังจากไม่มีกิจกรรมใด ๆ บนหน้าจอมากกว่า 10 นาที จัดเก็บเอกสารข้อมูลสำคัญขององค์กร รวมถึงข้อมูลที่อยู่ในสื่อบันทึกข้อมูลไว้ในสถานที่ที่สามารถปิดล็อค หรือเข้ารหัสข้อมูลดังกล่าวไว้ เจ้าหน้าที่ผู้ปฏิบัติงานจะต้องไม่ทิ้งเอกสารสำคัญไว้บนโต๊ะทำงาน และจัดเก็บโต๊ะทุกครั้งก่อนเลิกงาน ตรวจสอบทุกครั้งภายหลังการรับ-ส่งเอกสารทางเครื่องโทรสาร (Fax) ว่าไม่มีเอกสารสำคัญติดอยู่ที่เครื่องโทรสาร

---

# นโยบายการรักษาความมั่นคงปลอดภัยสารสนเทศ

## (6) ความมั่นคงปลอดภัยในการปฏิบัติงาน

## (Operations security)

### 6.1 ขั้นตอนการปฏิบัติงานและหน้าที่ความรับผิดชอบ (Operational procedures and responsibilities)

6.1.1 จัดทำเอกสารขั้นตอนการปฏิบัติงานให้ครอบคลุมการบริหารจัดการระบบสารสนเทศต่างๆ ภายในองค์กร เพื่อลดความผิดพลาดที่อาจเกิดขึ้นจากการปฏิบัติงาน

6.1.2 การบริหารการเปลี่ยนแปลง การเปลี่ยนแปลงใดๆ ในระบบเครือข่าย และระบบสารสนเทศขององค์กรจะต้องปฏิบัติตามขั้นตอนในระเบียบปฏิบัติ เรื่อง การบริหารการเปลี่ยนแปลง (รหัสเอกสาร PM-MS-05: Change management procedure)

6.1.3 การบริหารจัดการความต้องการทรัพยากรสารสนเทศในองค์กร ต้องมีการวางแผนตรวจสอบ เฝ้าระวังการใช้งานทรัพยากรสารสนเทศของอุปกรณ์ทั้งหมดที่มีอยู่ เพื่อให้สามารถรองรับความต้องการใช้งานที่อาจเพิ่มขึ้นได้ กำหนดระดับการแจ้งเตือนหากมีการใช้งานทรัพยากรสารสนเทศมากเกินกว่าระดับที่รองรับได้ (Threshold level) เพื่อให้สามารถดำเนินการแก้ไขได้ต่อไป โดยปฏิบัติตามขั้นตอนในระเบียบปฏิบัติ เรื่อง การบริหารจัดการขีดความสามารถ (รหัสเอกสาร PM-NW-06: Capacity management procedure)

6.1.4 การแบ่งแยกระบบสารสนเทศในการพัฒนา และทดสอบ เพื่อลดความผิดพลาดหรือผลกระทบอันเกิดจากการดำเนินการทดสอบใด ๆ โดยจะมีการแยกระบบสารสนเทศที่ให้บริการจริง ออกจากระบบสารสนเทศที่ใช้ในการพัฒนาและทดสอบ เพื่อลดความเสี่ยงจากการเข้าถึงโดยผู้ไม่มีสิทธิ์

### 6.2 การป้องกันโปรแกรมไม่ประสงค์ดี (Protection from malware)

6.2.1 มาตรการควบคุมโปรแกรมที่ไม่ประสงค์ดี (Malware)

6.2.1.1 แนวปฏิบัติสำหรับผู้ดูแลระบบ

1) เครื่องคอมพิวเตอร์แม่ข่ายและเครื่องคอมพิวเตอร์ส่วนบุคคลทุกเครื่องที่เชื่อมต่อกับระบบเครือข่ายจะต้องได้รับการติดตั้งโปรแกรมป้องกันไวรัส และจะต้องอัพเดท พร้อมทั้งปรับปรุงฐานข้อมูลรายชื่อไวรัส (virus definition file) ให้เป็นปัจจุบันอยู่เสมอ

2) เครื่องคอมพิวเตอร์แม่ข่ายและเครื่องคอมพิวเตอร์ที่เชื่อมต่ออยู่ในระบบเครือข่ายต้องทำการตรวจจับไวรัสอย่างสม่ำเสมอ
3) มีการแนะนำวิธีการใช้งานโปรแกรมตรวจจับไวรัสให้กับผู้ใช้งาน ในการฝึกอบรมประจำปี หรือประกาศผ่านอินทราเน็ต (Intranet) หรือช่องทางสื่อสารภายในองค์กร

6.2.1.2 แนวปฏิบัติสำหรับผู้ใช้งานระบบเครือข่าย

1) ผู้ใช้งานทุกคนจะต้องได้รับการอบรมให้เกิดความตระหนัก และเข้าใจถึงวิธีการในการอัพเดทโปรแกรมตรวจจับไวรัส
2) ห้ามผู้ใช้งานเครื่องคอมพิวเตอร์ที่เชื่อมต่ออยู่ในระบบเครือข่ายทำการเปิดแฟ้มข้อมูลที่อยู่ในสื่อบันทึกข้อมูลประเภทเคลื่อนย้ายได้ เช่น CD, DVD, USB, SD-Card โดยไม่ผ่านการ Scan virus ก่อน
3) ห้ามดาวน์โหลดโปรแกรมที่ละเมิดลิขสิทธิ์ลงในเครื่องคอมพิวเตอร์ที่เชื่อมต่อกับระบบเครือข่าย เพราะอาจมีสิ่งที่ไม่พึงประสงค์ติดมาด้วย
4) ห้ามเข้าเว็บไซต์ใด ๆ ที่จะก่อให้เกิดความเสี่ยงในการติดไวรัสในเครื่องคอมพิวเตอร์
5) อัพเดทโปรแกรมสแกนไวรัสที่เครื่องคอมพิวเตอร์ที่เข้าใช้งานอย่างสม่ำเสมอ
6) ห้ามกดรับไฟล์หรือเปิดลิงค์ที่ไม่รู้จักบนเครื่องคอมพิวเตอร์ที่ใช้งานภายในองค์กร
7) กรณีที่สงสัยว่าเครื่องติดไวรัสคอมพิวเตอร์ ให้รีบแจ้งผู้ดูแลระบบหรือผู้ได้รับมอบหมาย เพื่อดำเนินการแก้ไขอย่างเหมาะสมต่อไป

### 6.3 การสำรองข้อมูล (Backup)

6.3.1 วางแผนการสำรองข้อมูลของระบบสารสนเทศแต่ละระบบ กำหนดความถี่ในการสำรองข้อมูลพิจารณาตามความสำคัญของข้อมูลและความถี่ในการเปลี่ยนแปลงของข้อมูล กำหนดประเภทของข้อมูลที่ต้องทำการสำรองเก็บไว้ กำหนดรูปแบบการสำรองข้อมูลให้เหมาะสม โดยเป็นการสำรองข้อมูลแบบเต็ม (Full Backup) รวมทั้งบันทึกข้อมูลที่เกี่ยวข้องกับกิจกรรมการสำรองข้อมูล ได้แก่ ผู้ดำเนินการ วันและเวลา ชื่อข้อมูลที่สำรอง ผลการสำรองข้อมูล เป็นต้น โดยการดำเนินการให้เป็นไปตามขั้นตอนในระเบียบปฏิบัติ เรื่อง การสำรองข้อมูล (รหัสเอกสาร PM-SW-06)

6.3.2 ตรวจสอบข้อมูลทั้งหมดของระบบว่ามีการสำรองข้อมูลไว้อย่างครบถ้วน และหากพบว่าผิดปกติต้องจัดทำบันทึกและดำเนินการแก้ไขโดยทันที

6.3.3 กรณีที่จัดเก็บข้อมูลที่สำรองในสื่อบันทึกข้อมูล ต้องชี้บ่งสื่อบันทึกข้อมูลไว้อย่างชัดเจน โดยมีรายละเอียดของชื่อข้อมูล วันและเวลาที่สำรองข้อมูล ชื่อผู้รับผิดชอบ โดยสื่อสำรองข้อมูลจะต้องจัดเก็บไว้อย่างปลอดภัย และข้อมูลที่สำรองต้องเข้ารหัสเพื่อความปลอดภัย

6.3.4 จัดเก็บข้อมูลที่สำรองไว้นอกสถานที่ ระยะทางระหว่างสถานที่ที่จัดเก็บข้อมูลสำรองกับหน่วยงานต้องห่างกันเพียงพอ เพื่อไม่ให้ส่งผลกระทบต่อข้อมูลที่จัดเก็บไว้นอกสถานที่นั้นในกรณีที่เกิดภัยพิบัติกับหน่วยงาน เช่น ไฟไหม้น้ำท่วม แผ่นดินไหว การเกิดโรคระบาดจนไม่สามารถเข้ามาปฏิบัติงานในสถานที่ทำงานได้ เป็นต้น

6.3.5 วางแผนทดสอบบันทึกข้อมูลสำรองอย่างน้อยปีละ 1 ครั้ง ตามแผน BCP เพื่อตรวจสอบว่ายังคงสามารถเข้าถึงข้อมูลได้เป็นปกติ และสามารถนำข้อมูลที่สำรองกลับมาใช้งานได้ (restore) โดยการทดสอบต้องจัดทำบันทึกการทดสอบไว้เป็นหลักฐาน

## 6.4 การบันทึกข้อมูลการใช้งานและการเฝ้าระวัง (Logging and monitoring)

6.4.1 บันทึกเหตุการณ์ที่เกี่ยวข้องกับการใช้งานระบบสารสนเทศ (Event Logging) ผู้ดูแลระบบต้องดำเนินการจัดเก็บข้อมูลบันทึกเหตุการณ์ในระบบสารสนเทศให้สอดคล้องและครอบคลุมตามข้อกำหนดในพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.2560 มีการตรวจสอบบันทึกเหตุการณ์ในระบบสารสนเทศอย่างสม่ำเสมอ เพื่อตรวจสอบกิจกรรมที่มีแนวโน้มจะนำไปสู่การบุกรุกระบบหรือการดำเนินการใดๆ ที่อาจกระทบต่อความมั่นคงปลอดภัยของข้อมูลในองค์กรได้

6.4.2 ตรวจสอบการใช้งานระบบ (Monitoring System Use) ผู้ดูแลระบบควรมีการตรวจสอบการใช้งานระบบสารสนเทศอย่างสม่ำเสมอ เพื่อให้มั่นใจว่าระบบสารสนเทศยังคงสามารถให้บริการได้ตามปกติ และการใช้งานระบบต่างๆ ของผู้ใช้เป็นไปตามสิทธิ์ที่ได้รับ ตลอดจนเพื่อตรวจสอบความพยายามในการดำเนินการใดๆ ที่อาจกระทบต่อความมั่นคงปลอดภัยของข้อมูลในองค์กรได้ โดยควรเฝ้าระวังในประเด็นต่างๆ ตามขั้นตอนในระเบียบปฏิบัติ เรื่อง การติดตามการใช้งานระบบสารสนเทศ (รหัสเอกสาร PM-NW-05: Monitoring System Use Procedure)

6.4.3 การป้องกันบันทึกข้อมูลการใช้งานระบบสารสนเทศ (Protection of log information) อุปกรณ์และระบบที่ใช้ในการจัดเก็บบันทึกข้อมูลการใช้งานระบบสารสนเทศนั้น (Log information) จะต้องได้รับการป้องกันไม่ให้บุคคลที่ไม่เกี่ยวข้องสามารถเข้าไปเรียกดูข้อมูลหรือทำการแก้ไขได้ การเข้าถึงหรือใช้งานใดๆ ที่เกี่ยวข้องกับ log file นั้นจะต้องถูกบันทึกไว้ทุกครั้ง มีการตรวจสอบเนื้อที่ในการจัดเก็บ (Storage space) ข้อมูล Log file เพื่อให้มั่นใจว่ามีเนื้อที่เพียงพอที่จะจัดเก็บ log file ที่เป็นปัจจุบันอยู่ตลอดเวลา

6.4.4 ข้อมูลการใช้งานของผู้ดูแลระบบและผู้ปฏิบัติงาน (Administrator and Operator log) ต้องมีการบันทึกกิจกรรมการดำเนินการใดๆ ที่ใช้สิทธิ์ของผู้ดูแลระบบไว้ทุกครั้ง (เฉพาะระบบที่สามารถทำการบันทึกได้) และการดำเนินการใดๆ เกี่ยวข้องกับการจัดการผู้ใช้งานระบบ (User Management) ต้องมีการบันทึกไว้ทุกครั้งเช่นเดียวกัน

6.4.5 การบันทึกเหตุการณ์ที่เกิดจากความผิดพลาดจากระบบสารสนเทศ (Fault logging) ควรมีการบันทึกเหตุการณ์ใดๆ ที่เกิดจากความผิดพลาดหรือข้อบกพร่อง (Bug) ของระบบสารสนเทศทุกครั้ง เมื่อพบเหตุการณ์ในลักษณะดังกล่าวต้องเร่งหาสาเหตุพร้อมดำเนินการแก้ไขให้เหมาะสมเพื่อไม่ให้เกิดขึ้นอีกในอนาคตมาตรการหรือกลไกใด ๆ ที่นำมา

ใช้ในการแก้ไขปัญหาดังกล่าวต้องไม่ส่งผลกระทบต่อมาตรการด้านความมั่นคงปลอดภัยหรือกระทบต่อระบบสารสนเทศอื่นๆ ขององค์กร

6.4.6 การเทียบเวลามาตรฐาน (Clock Synchronization) การตั้งเวลาของเครื่องคอมพิวเตอร์ทุกเครื่องในหน่วยงาน ให้ตั้ง Time server ไปที่ time.windows.com เป็นที่เดียวกัน

## 6.5 การควบคุมการติดตั้งซอฟต์แวร์ปฏิบัติการ (Control of operational software)

6.5.1 การติดตั้งซอฟต์แวร์บนระบบปฏิบัติการ

6.5.1.1 โปรแกรมที่ติดตั้งลงบนเครื่องคอมพิวเตอร์ของหน่วยงานต้องเป็นโปรแกรมที่หน่วยงานได้ซื้อลิขสิทธิ์มาอย่างถูกต้องตามกฎหมาย ห้ามผู้ใช้งานคัดลอกโปรแกรมต่าง ๆ และนำไปติดตั้งบนเครื่องคอมพิวเตอร์ส่วนบุคคลหรือแก้ไข หรือนำไปให้ผู้อื่นใช้งานโดยผิดกฎหมาย

6.5.1.2 การติดตั้งโปรแกรมเป็นหน้าที่ของผู้ดูแลระบบ หากผู้ใช้งานต้องการใช้โปรแกรมอื่นนอกเหนือจากที่ลงไว้ให้ใช้งานในเครื่อง ต้องเป็นโปรแกรมที่มีลิขสิทธิ์ถูกต้อง หรือติดต่อผู้ดูแลระบบให้จัดหาโปรแกรมที่มีลิขสิทธิ์มาลงให้

## 6.6 การบริหารจัดการช่องโหว่ทางเทคนิค (Technical vulnerability management)

6.6.1 มีการเฝ้าระวังและติดตามประเมินความเสี่ยงสำหรับช่องโหว่ของระบบสารสนเทศ รวมทั้งดำเนินการประสานงานให้ผู้ที่เกี่ยวข้องดำเนินการแก้ไขช่องโหว่ตามความเหมาะสมโดยปฏิบัติตามขั้นตอนในระเบียบปฏิบัติ เรื่อง การจัดการช่องโหว่ทางเทคนิค (รหัสเอกสาร PM-SW-04: Patch management procedure)

6.6.2 มอบหมายผู้รับผิดชอบในการติดตามข่าวสารจากแหล่งข้อมูล เพื่อใช้ในการติดตามช่องโหว่ในระบบสารสนเทศขององค์กร

6.6.3 เมื่อพบช่องโหว่ในระบบสารสนเทศต้องรายงานหัวหน้างานเทคโนโลยีทางการศึกษาทราบเพื่อดำเนินการปิดช่องโหว่ดังกล่าว

6.6.4 จำกัดการแก้ไขเปลี่ยนแปลงใดๆ บนซอฟแวร์สำเร็จรูปที่ใช้ เพื่อลดโอกาสเสี่ยงของการเกิดช่องโหว่ของระบบ

## 6.7 การดำเนินการตรวจประเมินระบบสารสนเทศ (Information system audit considerations)

6.7.1 มาตรการควบคุมการตรวจประเมินระบบสารสนเทศ

6.7.1.1 ผู้ตรวจประเมินต้องแจ้งความต้องการ หรือแผนการตรวจประเมิน (ขอบเขต ระบบที่เข้าถึง สิทธิ์การดำเนินการ วันเวลา) โดยต้องได้รับอนุญาตจากผู้ช่วยคณบดีฝ่ายเทคโนโลยีทางการศึกษา และหากเป็นการประเมินจากภายนอก ต้องมีการทำข้อตกลงไม่เปิดเผยความลับ (NDA) ด้วย

6.7.1.2 การให้สิทธิ์การเข้าถึงระบบงานและข้อมูล ต้องถูกจำกัดสิทธิ์ให้สามารถอ่านได้อย่างเดียวเท่านั้น

6.7.1.3 ต้องมีการบันทึกกิจกรรมที่เกิดจากกระบวนการตรวจสอบระบบ (Logging) ทุกครั้ง (เฉพาะระบบที่สามารถทำการบันทึกได้)

6.7.1.4 กระบวนการตรวจสอบที่อาจส่งผลกระทบกับระบบงาน ต้องดำเนินการบนระบบทดสอบหรือนอกเวลาการให้บริการ (กรณีการตรวจสอบเชิงเทคนิคที่ต้องใช้สิทธิ์พิเศษ)

---

# นโยบายการรักษาความมั่นคงปลอดภัยสารสนเทศ

## (7) ความมั่นคงปลอดภัยด้านการสื่อสาร

## (Communication security)

### 7.1 การบริหารความมั่นคงปลอดภัยของระบบเครือข่าย (Network security management)

7.1.1 การควบคุมระบบเครือข่าย (Network control)

7.1.1.1 การระบุอุปกรณ์บนเครือข่าย (Equipment identification in network)

1) กำหนดให้ระบบสารสนเทศที่ต้องมีการควบคุมการเข้าถึง โดยระบุ IP Address และ MAC Address
2) การติดตั้งและการเชื่อมต่ออุปกรณ์เครือข่ายจะต้องดำเนินการโดยเจ้าหน้าที่งานเทคโนโลยีทางการศึกษาหรือผู้ที่ได้รับอนุญาตเท่านั้น
3) ต้องใช้ไฟร์วอลล์ (Firewall) ที่สามารถกำหนด IP Address และ MAC Address ที่จะเข้าถึงเครือข่ายของหน่วยงานได้
4) จัดทำแผนผังระบบเครือข่าย ซึ่งประกอบด้วย รายละเอียดที่เกี่ยวกับขอบเขตของเครือข่ายภายในและเครือข่ายภายนอก พร้อมทั้งระบุอุปกรณ์ที่ติดตั้งในระบบเครือข่าย
5) แผนผังเครือข่าย เป็นเอกสารในระดับลับมากจะต้องจัดเก็บอย่างปลอดภัย ควบคุมการเผยแพร่ และทบทวนแผนผังระบบเครือข่ายพร้อมอุปกรณ์ที่ติดตั้งให้เป็นปัจจุบันอยู่เสมออย่างน้อยปีละ 1 ครั้ง

7.1.1.2 การใช้งานพอร์ตที่ใช้สำหรับการตรวจสอบและปรับแต่งระบบ

1) การใช้งานพอร์ตสำหรับตรวจสอบและปรับแต่งระบบ ต้องมีการขออนุญาต ให้เข้าถึงได้เฉพาะผู้ที่ได้รับอนุญาตเท่านั้น
2) มีการป้องกันโดยการปิดบริการ (Services) การเข้าถึงช่องทางที่ใช้บำรุงรักษาระบบผ่านเครือข่าย และเปิดใช้เฉพาะอุปกรณ์และเวลาที่จำเป็นเท่านั้น
3) ปิดการใช้งาน หรือควบคุมการเข้าถึงพอร์ตที่ใช้สำหรับตรวจสอบและปรับแต่งระบบให้ใช้งานได้ โดยจำกัดระยะเวลาเท่าที่จำเป็น
4) ติดตั้งเครื่องมือตรวจจับและป้องกันการบุกรุกทางเครือข่าย

7.1.1.3 การควบคุมการเชื่อมต่อทางเครือข่าย

1) กำหนดสิทธิ์ของผู้ใช้งานในการเชื่อมต่อเข้าสู่ระบบเครือข่าย โดยอนุญาตให้ผู้ใช้สามารถนำอุปกรณ์ส่วนตัวมาเชื่อมต่อระบบเครือข่ายได้ไม่เกินคนละ 3 เครื่องเท่านั้น โดยการเปิดสิทธิ์จะปฏิบัติตามขั้นตอนในระเบียบปฏิบัติ เรื่อง การบริหารจัดการสิทธิ์ผู้ใช้งาน (รหัสเอกสาร PM-NW-01)
2) ระบบเครือข่ายต้องเชื่อมต่อผ่านอุปกรณ์ป้องกันการบุกรุก (Firewall, IDS/IPS) ที่ผู้ดูแลระบบทำการติดตั้งและติดตามเฝ้าระวังอยู่
3) การเข้าสู่ระบบเครือข่ายของหน่วยงานต้องเข้าสู่ระบบผ่านช่องทางที่ปลอดภัยที่กำหนดไว้เท่านั้น
4) ห้ามผู้ใดกระทำการเคลื่อนย้าย ติดตั้งเพิ่มเติมหรือทำการใด ๆ ต่ออุปกรณ์ส่วนกลาง ได้แก่ อุปกรณ์จัดเส้นทาง (Router) อุปกรณ์กระจายสัญญาณข้อมูล (Switch) อุปกรณ์ที่เชื่อมต่อกับระบบเครือข่ายหลัก โดยไม่ได้รับอนุญาตจากผู้ดูแลระบบ

7.1.1.4 การควบคุมการจัดเส้นทางบนเครือข่าย

1) ควบคุมไม่ให้มีการเปิดเผยแผนการใช้หมายเลขเครือข่าย (IP Address)
2) กำหนดให้มีการแปลงหมายเลขเครือข่ายและชื่อโดเมน เพื่อแยกเครือข่ายย่อย เครือข่ายภายในและภายนอก
3) กำหนดตารางการใช้เส้นทางบนระบบเครือข่าย บนอุปกรณ์จัดเส้นทาง (Router) หรืออุปกรณ์กระจายสัญญาณเพื่อควบคุมผู้ใช้งานเฉพาะเส้นทางที่ได้รับอนุญาตเท่านั้น

7.1.1.5 การควบคุมระบบเครือข่ายไร้สาย (Wireless LAN Access Control)

1) กำหนดสิทธิ์ของผู้ใช้งานในการเชื่อมต่อเข้าสู่ระบบเครือข่ายไร้สาย โดยอนุญาตให้ผู้ใช้สามารถนำอุปกรณ์ส่วนตัวมาเชื่อมต่อระบบเครือข่ายไร้สายได้ไม่เกินคนละ 3 เครื่องเท่านั้น โดยการกำหนดสิทธิ์จะขึ้นอยู่กับกลุ่มผู้ใช้งาน ดังนี้
    - บุคลากรภายในคณะ ให้กำหนดสิทธิ์โดยปฏิบัติตามขั้นตอนในระเบียบปฏิบัติ เรื่อง การบริหารจัดการสิทธิ์ผู้ใช้งาน (รหัสเอกสาร PM-NW-01)
    - บุคคลภายนอกคณะที่ขอเข้าใช้งานระบบเครือข่ายไร้สายของคณะ ให้กำหนดสิทธิ์โดยปฏิบัติตามขั้นตอนในระเบียบปฏิบัติ เรื่อง การขอเปิดสิทธิ์ชั่วคราวเพื่อใช้งานเครือข่ายสำหรับบุคคลภายนอก (รหัสเอกสาร PM-NW-02)

2) ต้องควบคุมสัญญาณของอุปกรณ์กระจายสัญญาณ (Access Point) เพื่อป้องกันไม่ให้สัญญาณของอุปกรณ์รั่วไหลออกนอกพื้นที่ใช้งานระบบเครือข่ายไร้สาย และป้องกันไม่ให้ผู้โจมตีสามารถรับส่งสัญญาณจากภายนอกอาคารหรือบริเวณขอบเขตที่ควบคุมได้
3) ดำเนินการเปลี่ยนค่า SSID (Service Set Identifier) ที่ถูกกำหนดเป็นค่า Default มาจากผู้ผลิตทันทีที่นำอุปกรณ์กระจายสัญญาณ (Access Point) มาใช้งาน
4) เปลี่ยนค่าชื่อบัญชีรายชื่อและรหัสผ่านในการเข้าสู่ระบบสำหรับการตั้งค่าการทำงานของอุปกรณ์ไร้สายและเลือกใช้ชื่อบัญชีรายชื่อและรหัสผ่านที่คาดเดาได้ยาก เพื่อป้องกันไม่ให้ผู้โจมตีสามารถคาดเดาหรือเจาะรหัสได้โดยง่าย
5) เลือกใช้วิธีการควบคุมการเข้าถึงโดยผ่านหน้าระบบการยืนยันตัวตน (Authentication) ด้วยชื่อผู้ใช้ (Username) และรหัสผ่าน (Password) ของผู้ใช้งานที่มีสิทธิในการเข้าใช้งานระบบเครือข่ายไร้สาย
6) ใช้ซอฟต์แวร์หรือฮาร์ดแวร์เพื่อตรวจสอบความมั่นคงปลอดภัยของระบบเครือข่ายไร้สายอย่างสม่ำเสมอ เพื่อตรวจสอบและบันทึกเหตุการณ์ที่น่าสงสัยที่เกิดขึ้นในระบบเครือข่ายไร้สาย และเมื่อตรวจสอบพบการใช้งานระบบเครือข่ายไร้สายที่ผิดปกติให้รายงานต่อหัวหน้างานเทคโนโลยีทางการศึกษาทันที

7.1.2 ความมั่นคงปลอดภัยของบริการเครือข่าย (Security of network services)

6.1.2.1 การเข้าถึงระบบเครือข่าย

1) กำหนดให้ผู้ใช้งานสามารถเข้าถึงระบบเครือข่ายได้เฉพาะระบบเครือข่ายที่ได้รับอนุญาตเท่านั้น
2) จำกัดการใช้เส้นทางบนเครือข่ายจากเครื่องคอมพิวเตอร์ไปยังเครื่องคอมพิวเตอร์แม่ข่ายเพื่อไม่ให้ผู้ใช้งานสามารถใช้เส้นทางอื่น ๆ ได้
3) ระบบเครือข่ายทั้งหมดของหน่วยงานที่มีการเชื่อมต่อไปยังระบบเครือข่ายภายนอกหน่วยงานต้องเชื่อมต่อผ่านอุปกรณ์ป้องกันการบุกรุก รวมทั้งต้องมีความสามารถในการตรวจจับโปรแกรมไม่ประสงค์ดี (Malware) ทั้งหลายด้วย
4) ระบบเครือข่ายต้องติดตั้งระบบตรวจจับการบุกรุก (Intrusion Prevention System IPS/ Intrusion Detection System IDS) เพื่อตรวจสอบการบุกรุกผ่านระบบเครือข่าย การเข้าใช้งานระบบเครือข่ายของหน่วยงานในลักษณะที่ผิดปกติ และการแก้ไขเปลี่ยนแปลงระบบเครือข่ายโดยบุคคลที่ไม่มีอำนาจหน้าที่เกี่ยวข้อง

5) กำหนดการป้องกันเครือข่ายและอุปกรณ์ต่าง ๆ ที่เชื่อมต่อกับระบบเครือข่ายอย่างชัดเจน และต้องทบทวนการกำหนดค่า Parameter ต่าง ๆ เช่น IP Address อย่างน้อยปีละ 2 ครั้ง หากมีการแก้ไขหรือเปลี่ยนแปลงค่า Parameter ต้องแจ้งบุคคลที่เกี่ยวข้องให้รับทราบทุกครั้ง

6) IP address ของระบบงานเครือข่ายภายในต้องมีการป้องกันมิให้หน่วยงานภายนอกที่เชื่อมต่อสามารถมองเห็นได้ เพื่อเป็นการป้องกันไม่ให้บุคคลภายนอกสามารถรู้ข้อมูลเกี่ยวกับโครงสร้างของระบบเครือข่ายได้โดยง่าย

7) การใช้เครื่องมือต่าง ๆ (Tools) เพื่อการตรวจสอบระบบเครือข่าย ต้องได้รับการอนุมัติจากผู้ดูแลระบบ และจำกัดการใช้งานเฉพาะเท่าที่จำเป็น

8) การใช้งานระบบสารสนเทศที่สำคัญ เช่น ระบบคอมพิวเตอร์, โปรแกรมประยุกต์ (Application), ระบบเครือข่ายไร้สาย (Wireless LAN), ระบบอินเทอร์เน็ต (Internet) และระบบปฏิบัติงานภายในองค์กร (intranet) เป็นต้น โดยต้องให้สิทธิ์เฉพาะ การปฏิบัติงานในหน้าที่ และต้องได้รับความเห็นชอบจากผู้บังคับบัญชา รวมทั้งต้องทบทวนสิทธิ์ดังกล่าวอย่างน้อยปีละ 1 ครั้ง

7.1.2.2 การยืนยันตัวบุคคลสำหรับผู้ใช้งานที่อยู่ภายนอกองค์กร

1) ผู้ใช้งานที่อยู่ภายนอกองค์กร เมื่อต้องเข้าใช้งานระบบสารสนเทศต้องแสดงตัวตน (Identification) ด้วยชื่อผู้ใช้งาน (Username) ทุกครั้ง

2) มีการตรวจสอบผู้ใช้งานทุกครั้งก่อนที่จะอนุญาตให้เข้าถึงระบบข้อมูล โดยจะต้องมีวิธีการยืนยันตัวบุคคล (Authentication) เพื่อแสดงว่าเป็นผู้ใช้งานตัวจริงด้วยการใช้รหัสผ่าน (Password)

3) หากจำเป็นต้องเข้าสู่ระบบเครือข่ายของคณะจากเครือข่ายภายนอก ต้องมีการเข้ารหัสที่เป็นมาตรฐานสากลเพื่อความมั่นคงปลอดภัยด้วยวิธี VPN โดยต้องได้รับอนุญาตจากหัวหน้างานเทคโนโลยีทางการศึกษาก่อน โดยปฏิบัติตามขั้นตอนในระเบียบปฏิบัติ เรื่อง การให้บริการ VPN สำหรับบุคคลภายนอก (รหัสเอกสาร PM-NW-04)

7.1.3 การแบ่งแยกเครือข่าย (Segregation in network) โดยแบ่งออกเป็น 2 เครือข่ายตามลักษณะการใช้งาน ดังนี้

1) เครือข่ายไร้สาย เป็นเครือข่ายที่อำนวยความสะดวกในการทำงานด้วยอุปกรณ์พกพาต่าง ๆ เครือข่ายนี้สามารถใช้งานอินเทอร์เน็ตได้แต่ไม่สามารถเข้าถึงทรัพยากรที่ใช้ร่วมกันบนเครือข่ายหลักได้ โดยแบ่งเป็น 2 กลุ่มตามผู้ใช้งาน

- บุคลากรภายในคณะ ใช้งานผ่านเครือข่าย SSID ชื่อ MED และ MED5G
- บุคคลภายนอก เช่น ผู้มาติดต่องาน หรือผู้เข้ารับการอบรม สามารถใช้บริการอินเทอร์เน็ตเป็นการชั่วคราวได้ โดยผ่านเครือข่ายสำหรับผู้ใช้งานภายนอก SSID ชื่อ MED-GUEST และ MED5G-GUEST

2) เครือข่ายภายใน เป็นการเชื่อมต่อคอมพิวเตอร์สำนักงานของหน่วยงานต่าง ๆ ในคณะเข้ากับ server และอินเทอร์เน็ตภายนอก โดยได้มีการจัดแบ่งออกเป็น zone เพื่อสะดวกต่อการบริหารจัดการตามความเหมาะสมของการใช้งานในแต่ละ zone ดังนี้
   - Internal zone เป็น Network zone ของคอมพิวเตอร์สำนักงานที่บุคลากรใช้ในการปฏิบัติงาน มีการเชื่อมต่อกับสัญญาณอินเทอร์เน็ตภายนอกผ่าน Firewall
   - Demilitarized zone (DMZ) เป็น Network Zone ที่มี Web Application Server ต่าง ๆ ของคณะอยู่ มีการเชื่อมต่อกับสัญญาณอินเทอร์เน็ตภายนอกผ่าน Firewall และบุคคลภายนอกสามารถใช้งานได้ผ่านทาง Web browser
   - Database zone เป็น Network zone ที่มี Database Server ของคณะอยู่ และมีการเชื่อมต่อกับ Web Application Server เท่านั้น โดยไม่มีการเชื่อต่อกับอินเทอร์เน็ตภายนอกเลย

---

# นโยบายการรักษาความมั่นคงปลอดภัยสารสนเทศ

## (8) การจัดหา พัฒนา และบำรุงรักษาระบบ

## (System acquisition, development and maintenance)

### 8.1 ข้อกำหนดด้านความมั่นคงปลอดภัยของระบบสารสนเทศ

8.1.1 การวิเคราะห์และกำหนดความต้องการด้านความมั่นคงปลอดภัยสารสนเทศ

ในการจัดหาอุปกรณ์ หรือระบบต่างๆ เพื่อนำมาใช้ในองค์กรนั้น ต้องมีการพิจารณาองค์ประกอบด้านความมั่นคงปลอดภัยของอุปกรณ์หรือเทคโนโลยีต่างๆร่วมด้วย เพื่อลดความเสียหายที่เกิดจากระบบไม่สามารถรองรับปริมาณความต้องการใช้งานหรือไม่สามารถปฏิบัติตามข้อกำหนดด้านความมั่นคงปลอดภัยขององค์กรได้ ในการพิจารณาต้องให้ครอบคลุมประเด็นต่างๆ ดังนี้

8.1.1.1 ระบบปฏิบัติการ ต้องมีองค์ประกอบในการจัดการระบบ ได้แก่

1) การอนุมัติและการพิสูจน์ตัวตนของผู้ใช้งาน
2) การตั้งค่าระบบและการกำหนดบริการต่าง ๆ ที่มีในระบบ
3) การตรวจสอบและเฝ้าระวังระบบ โดยมีการจัดเก็บ log ของกิจกรรมต่าง ๆ ในระบบให้สอดคล้องกับข้อกำหนดตามกฎหมาย

8.1.1.2 ระบบแอพพลิเคชั่น ต้องมีองค์ประกอบในการจัดการบนแอพลิเคชั่น ได้แก่

1) การอนุมัติและการพิสูจน์ตัวตนของผู้ใช้งาน
2) การจัดการสิทธิ์การเข้าใช้ข้อมูลสารสนเทศในระบบ
3) การตั้งค่าของข้อมูลสารสนเทศ ให้สามารถกำหนดระดับชั้นความลับของข้อมูล และมาตรการป้องกันต่างๆ
4) การตั้งค่าบนระบบแอพลิเคชั่น และการกำหนดบริการต่าง ๆ ที่มีในระบบแอพลิเคชั่น
5) การตรวจสอบและเฝ้าระวังระบบแอพลิเคชั่น โดยมีการจัดเก็บ log ของการเพิ่มและแก้ไขข้อมูลในระบบให้สอดคล้องกับข้อกำหนดตามกฎหมาย
6) หากเกิดภัยพิบัติสามารถกู้คืนระบบได้

8.1.1.3 ระบบโครงสร้างพื้นฐาน สามารถรองรับการตั้งค่าต่าง ๆ ตามที่กำหนดในระดับชั้นความลับ รองรับการให้บริการอย่างต่อเนื่อง หากเกิดภัยพิบัติสามารถกู้คืนระบบได้ หรือมีมาตรการต่างๆ ในการกู้ระบบสอดคล้อง

กับข้อกำหนดตามกฎหมาย โดยต้องมีการตรวจสอบความถูกต้องในการติดตั้งระบบและการทำงานของระบบในช่วงที่มีการพัฒนาระบบร่วมกับผู้เชี่ยวชาญด้านความมั่นคงปลอดภัย เพื่อให้มั่นใจว่าได้มีการประเมินแล้วว่าระบบได้ถูกออกแบบและพัฒนาอย่างเหมาะสมเป็นไปตามข้อกำหนดด้านความมั่นคงปลอดภัยที่ได้กำหนดไว้

8.1.2 ความมั่นคงปลอดภัยของการใช้บริการบนเครือข่ายสาธารณะ

8.1.2.1 ห้ามใช้ระบบอินเทอร์เน็ต (Internet) ของหน่วยงาน เพื่อหาประโยชน์ในเชิงพาณิชย์เป็นการส่วนบุคคล และทำการเข้าสู่เว็บไซต์ที่ไม่เหมาะสมขัดต่อศีลธรรม เว็บไซต์ที่เป็นภัยต่อสังคมหรือละเมิดสิทธิ์ของผู้อื่น หรือข้อมูลที่อาจก่อให้เกิดความเสียหายให้กับหน่วยงาน/องค์กร

8.1.2.2 ไม่เปิดเผยข้อมูลสำคัญที่เป็นความลับเกี่ยวกับงานของหน่วยงาน หรือข้อมูลเฉพาะส่วนตัวผ่านระบบอินเทอร์เน็ต (Internet)

8.1.2.3 ระมัดระวังการดาวน์โหลดโปรแกรมใช้งานจากระบบอินเทอร์เน็ต ต้องเป็นไปโดยไม่ละเมิดลิขสิทธิ์ หรือทรัพย์สินทางปัญญา

8.1.2.4 ไม่เสนอความคิดเห็น หรือใช้ข้อความที่ ยั่วยุ ให้ร้าย ที่จะทำให้เกิดความเสื่อมเสียต่อชื่อเสียงของหน่วยงาน การทำลายความสัมพันธ์กับบุคลากรของหน่วยงานอื่น ๆ ผ่านระบบอินเทอร์เน็ต (Internet)

8.1.2.5 ผู้ใช้งานไม่นำเข้าข้อมูลคอมพิวเตอร์ใด ๆ ที่มีลักษณะอันเป็นเท็จ อันเป็นความผิด เกี่ยวกับความมั่นคงแห่งราชอาณาจักร อันเป็นความผิดเกี่ยวกับการก่อการร้าย หรือภาพที่มีลักษณะลามก และไม่ทำการเผยแพร่หรือส่งต่อข้อมูลคอมพิวเตอร์ดังกล่าวผ่านอินเทอร์เน็ต

8.1.2.6 หลังจากใช้งานระบบอินเทอร์เน็ต (Internet) เสร็จแล้ว ให้ปิดเว็บเบราเซอร์ (Web Browser) และออกจากระบบเพื่อป้องกันการเข้าใช้งานโดยบุคคลอื่น ๆ

8.1.2.7 ผู้ใช้งานต้องปฏิบัติตามกฎหมายว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ อย่างเคร่งครัด

## 8.2 ความมั่นคงปลอดภัยในกระบวนการพัฒนาและสนับสนุน

8.2.1 นโยบายความปลอดภัยในการพัฒนาระบบ

8.2.1.1 การพัฒนาซอฟต์แวร์และระบบสารสนเทศต้องวางแผนและระบุองค์ประกอบต่างๆที่จำเป็นและข้อกำหนด ด้านความมั่นคงปลอดภัยของระบบงานที่จะจัดหา หรือพัฒนาขึ้นไว้ให้ชัดเจนเป็นลายลักษณ์อักษร

8.2.1.2 ดำเนินการพัฒนาหรือจัดหาระบบงานให้ได้ตามข้อกำหนดของระบบงาน และข้อกำหนดด้านความมั่นคงปลอดภัยตามที่ได้ระบุไว้

8.2.1.3 ระบบงานที่จัดหาหรือพัฒนาขึ้นต้องมีฟังก์ชันสำหรับผู้ดูแลระบบเพื่อทำการบันทึกและปรับเปลี่ยนสิทธิ์ของผู้ใช้งานได้ รวมทั้งต้องสามารถบันทึกสิทธิ์ดังกล่าวลงเก็บไว้ในฐานข้อมูลได้ด้วย

8.2.1.4 การติดตั้งหรือปรับปรุงซอฟต์แวร์ของระบบงานต้องมีการขออนุมัติให้ติดตั้งก่อนดำเนินการ

8.2.1.5 ผู้รับผิดชอบระบบสารสนเทศของหน่วยงานต้องควบคุมการติดตั้งซอฟต์แวร์ลงไปยังระบบเครื่องคอมพิวเตอร์ที่ให้บริการ

8.2.2 กระบวนการควบคุมการเปลี่ยนแปลง

8.2.2.1 ให้มีการควบคุมการเปลี่ยนแปลงต่อระบบงานของหน่วยเพื่อป้องกันความเสียหายหรือการหยุดชะงักที่มีต่อระบบงานนั้น

8.2.2.2 ให้ผู้ดูแลระบบที่ได้รับการอบรมแล้ว หรือมีความชำนาญเท่านั้น ที่จะเป็นผู้ทำหน้าที่ดำเนินการเปลี่ยนแปลงต่อระบบงานของหน่วยงาน

8.2.3 การทบทวนทางเทคนิคของแอพพลิเคชั่นหลังจากที่มีการเปลี่ยนแปลงโครงสร้างพื้นฐานของระบบ กำหนดให้ผู้รับผิดชอบระบบสารสนเทศต้องดำเนินการดังนี้

8.2.3.1 แจ้งให้ผู้ที่เกี่ยวข้องกับระบบงานได้รับทราบเกี่ยวกับการเปลี่ยนแปลงโครงสร้างพื้นฐานของระบบ เพื่อให้บุคคลเหล่านั้นมีเวลาเพียงพอในการดำเนินการทดสอบและทบทวนแอพพลิเคชั่น ก่อนที่จะดำเนินการเปลี่ยนแปลงระบบ

8.2.3.2 พิจารณาวางแผนดำเนินการเปลี่ยนแปลงโครงสร้างพื้นฐานของระบบงานรวมทั้งวางแผนด้านงบประมาณ ที่จำเป็นต้องใช้ ในกรณีที่ต้องเปลี่ยนไปใช้ระบบปฏิบัติการใหม่

8.2.4 จำกัดการเปลี่ยนแปลงบนซอฟต์แวร์แพ็คเกจ

8.2.4.1 ห้ามทำการเปลี่ยนแปลงใดๆบนซอฟต์แวร์สำเร็จรูปยกเว้นจะได้รับอนุญาตจากผู้บริหารก่อน

8.2.4.2 จำกัดการติดตั้งโปรแกรมแก้ไขช่องโหว่ต่างๆ (Patch) ที่เกี่ยวข้องกับระบบงานตามความจำเป็น เช่น โปรแกรมแก้ไขช่องโหว่สำหรับระบบปฏิบัติการ โปรแกรมแก้ไขช่องโหว่สำหรับระบบบริหารจัดการฐานข้อมูล เป็นต้น

8.2.4.3 ตรวจสอบและปิดพอร์ต (Port) บนระบบงานที่ไม่มีความจำเป็นในการใช้งาน ก่อนเปิดระบบให้บริการ

8.2.4.4 จัดให้มีการป้องกันไวรัสคอมพิวเตอร์บนระบบงานที่ทำการติดตั้ง

8.2.4.5 จำกัดการเชื่อมต่อทางเครือข่าย การเข้าถึง source code อนุญาตให้เฉพาะกลุ่มผู้ใช้งาน ที่เกี่ยวข้องเท่านั้น

8.2.5 หลักการด้านวิศวกรรมระบบความปลอดภัย

การจัดหา หรือพัฒนาซอฟต์แวร์ ต้องดำเนินการตามมาตรฐานวิศวกรรมซอฟต์แวร์ที่ครบวงจร เพื่อให้ระบบมีการพัฒนาอย่างต่อเนื่อง โดยมีขั้นตอนการพัฒนาพื้นฐานจัดทำเป็นเอกสารไว้ ดังนี้

8.2.5.1 การวิเคราะห์ระบบงาน (Analysis) มีการเก็บข้อมูลของระบบงาน และความต้องการของผู้ใช้ (User Requirements) มีบันทึกความต้องการของระบบอย่างชัดเจน

8.2.5.2 การออกแบบระบบ (Design) มีการออกแบบฐานข้อมูลและตารางที่มีความสัมพันธ์ รวมทั้งส่วนที่ติดต่อกับผู้ใช้งาน

8.2.5.3 การโปรแกรมระบบ (Coding) มีการเขียนและพัฒนาโปรแกรมตามการออกแบบ โดยยึดหลักการพัฒนาที่แบ่งระบบออกเป็นโมดูล หรือฟังก์ชัน เพื่อให้ง่ายต่อการติดตามและแก้ไข รวมทั้งมีคำแนะนำอธิบายภายในโปรแกรมประกอบ

8.2.5.4 การทดสอบระบบ (Testing) เพื่อทดสอบการใช้งานระบบ เป็นการทดสอบทั้งความถูกต้องของการทำงาน และค้นหาข้อผิดพลาด (Errors) ที่อาจเกิดขึ้นในโปรแกรมระบบ รวมทั้งรายงานผลการทดสอบใช้งาน

8.2.5.5 การออกแบบระบบการรักษาความปลอดภัย (Security Operational Design) เพื่อให้การใช้งานซอฟต์แวร์ที่พัฒนาขึ้นมาใช้งานในระบบที่มีความปลอดภัย ป้องการการโจมกรรมข้อมูล หรือ การโจมตีระบบผ่านทางเครือข่าย ผู้พัฒนาต้องติดตามและแก้ไขโปรแกรม/ระบบงาน ให้มีความปลอดภัย ปราศจากช่องโหว่ที่เกิดจากระบบปฏิบัติการเครื่องแม่ข่าย และโปรแกรมระบบงานที่พัฒนาขึ้นมา

8.2.6 การพัฒนาซอฟต์แวร์โดยหน่วยงานภายนอก

8.2.6.1 กำหนดให้มีการควบคุมโครงการพัฒนาซอฟต์แวร์โดยผู้ให้บริการจากภายนอก

8.2.6.2 ต้องระบุว่าใครจะเป็นผู้มีสิทธิ์ในทรัพย์สินทางปัญญาสำหรับซอร์สโค้ด ในการพัฒนาซอฟต์แวร์โดยผู้ให้บริการจากภายนอก

8.2.6.3 กำหนดเรื่องการสงวนสิทธิ์ที่จะตรวจสอบด้านคุณภาพและความถูกต้องของซอฟต์แวร์ที่จะมีการพัฒนาโดยผู้ให้บริการภายนอก โดยระบุไว้ในสัญญาจ้างที่ทำกับผู้ให้บริการภายนอกนั้น

8.2.6.4 กำหนดให้มีการตรวจสอบโปรแกรมไม่ประสงค์ดี ในซอฟต์แวร์ต่างๆ ก่อนมีการติดตั้ง

8.2.7 การทดสอบความปลอดภัยของระบบ

8.2.7.1 กำหนดให้ผู้ใช้งาน หรือผู้ที่เกี่ยวข้องต้องทำการทดสอบระบบงานตามจุดประสงค์ที่กำหนดไว้อย่างครบถ้วน เพียงพอ ก่อนดำเนินการติดตั้งบนเครื่องที่ให้บริการระบบงานจริง ได้แก่ ซอฟต์แวร์ระบบปฏิบัติการ ซอฟต์แวร์ที่พัฒนาขึ้นใช้ในระบบงาน เป็นต้น

8.2.7.2 ผู้ที่เกี่ยวข้องต้องทำการทดสอบด้านความมั่นคงปลอดภัยของระบบงานอย่างครบถ้วนก่อนดำเนินการติดตั้งบนเครื่องที่ให้บริการระบบงานจริง

8.2.7.3 ทำการปรับปรุงไลบรารี่สำหรับซอฟต์แวร์ของระบบงานให้มีความทันสมัยและสอดคล้องกับระบบที่ติดตั้ง

8.2.7.4 กรณีที่เป็นการติดตั้งระบบเพื่อทดแทนระบบงานเดิม ให้ทำการสำรองข้อมูลที่จำเป็น เช่น ฐานข้อมูลซอฟต์แวร์ ค่าคอนฟิกกูเรชัน หรืออื่นๆ ที่เกี่ยวข้องกับระบบงานนั้น หากการติดตั้งทำไม่สำเร็จจะได้สามารถกลับไปใช้ระบบงานเดิมได้

8.2.7.5 กรณีที่มีความจำเป็นต้องถ่ายโอนข้อมูลในระบบงานเดิมไปสู่ข้อมูลในระบบงานที่จะทำการติดตั้ง ให้กำหนดแผนการถ่ายโอนข้อมูลจากระบบงานเดิมไปสู่ระบบงานใหม่ ทำการถ่ายโอนข้อมูลตามแผน โดยดำเนินการร่วมกับผู้ใช้งานเพื่อตรวจสอบว่าข้อมูลที่มีการถ่ายโอนไปนั้นมีความถูกต้องและครบถ้วนหรือไม่

8.2.7.6 กำหนดแผนการติดตั้งสำหรับระบบงานซึ่งรวมถึงระยะเวลาที่จะดำเนินการรวมทั้งแจ้งให้ผู้ที่เกี่ยวข้องได้รับทราบก่อนล่วงหน้า เช่น แผนการติดตั้งฮาร์ดแวร์ ซอฟต์แวร์ และอื่น ๆ

8.2.7.7 สำหรับซอฟต์แวร์ที่จะทำการติดตั้ง ต้องทำการตรวจสอบให้แน่ใจว่าจะไม่เป็นการละเมิดลิขสิทธิ์ของผู้ผลิตซอฟต์แวร์นั้น

8.2.7.8 ให้อ่านและปฏิบัติตามเงื่อนไขหรือข้อตกลงการใช้งานซอฟต์แวร์ที่ทำการติดตั้งอย่างเคร่งครัด

8.2.7.9 สำหรับการติดตั้งซอฟต์แวร์ยูทิลิตี้ (Utility Software) ต้องตรวจสอบก่อนว่าเป็นซอฟต์แวร์ที่มีการทำงานที่ถูกต้องและเชื่อถือได้

8.2.8 การทดสอบเพื่อการยอมรับระบบ

8.2.8.1 กำหนดให้มีการจัดทำแผนการทดสอบ

8.2.8.2 กำหนดเกณฑ์ในการตรวจรับให้ชัดเจนโดยผู้พัฒนาระบบ

8.2.8.3 ทำการทดสอบตามแผนที่กำหนด และบันทึกผลการทดสอบ

8.2.8.4 รายงานผลการทดสอบให้ผู้บังคับบัญชารับทราบเพื่อให้คำแนะนำในการปรับปรุงที่จำเป็น

**8.3 ข้อมูลทดสอบ**

8.3.1 ไม่อนุญาตให้นำข้อมูลสำคัญขององค์กรไปใช้ในการทดสอบกับระบบที่พัฒนาหรือปรับปรุงใหม่ เพื่อป้องกัน การรั่วไหลของข้อมูล เว้นเสียแต่ได้รับการอนุมัติจากผู้บริหารระดับสูงก่อน และหากเป็นไปได้ให้ตัดข้อมูลส่วนที่สำคัญทิ้งไป ให้เหลือเฉพาะส่วนที่เพียงพอต่อการนำไปใช้ในการทดสอบ

8.3.2 การทดสอบซอฟต์แวร์ ห้ามทดสอบบนระบบและฐานข้อมูลที่ใช้งานจริง ต้องทำการสำรองระบบและข้อมูลเพื่อใช้ในการทดสอบ เพื่อป้องกันความเสียหายที่อาจจะเกิดขึ้นได้กับระบบที่ใช้งานอยู่

---

# นโยบายการรักษาความมั่นคงปลอดภัยสารสนเทศ

## (9) ความสัมพันธ์กับผู้ให้บริการภายนอก

## (Supplier relationships)

### 9.1 ความมั่นคงปลอดภัยสารสนเทศที่สัมพันธ์กับผู้ให้บริการภายนอก

9.1.1 ผู้ให้บริการภายนอกที่สามารถเข้าปฏิบัติภารกิจเกี่ยวข้องระบบสารสนเทศขององค์กรได้จะต้องเป็นผู้ให้บริการที่ผ่านการคัดเลือกตามกระบวนการจัดซื้อจัดจ้างขององค์กรเท่านั้น

9.1.2 ผู้ให้บริการภายนอกที่ต้องการสิทธิ์ในการเข้าถึงระบบสารสนเทศของหน่วยงาน และการเข้าปฏิบัติงานต้องทำเรื่องขออนุญาตเป็นลายลักษณ์อักษรเพื่อขออนุมัติจากผู้ช่วยคณบดีฝ่ายเทคโนโลยีทางการศึกษา และมีการลงนามในสัญญาการรักษาความลับและไม่เปิดเผยข้อมูลของหน่วยงาน (NDA) ที่มีผลทางกฎหมายแม้สิ้นสุดโครงการ

9.1.3 ผู้ให้บริการภายนอกที่ได้รับสิทธิ์เข้าใช้งานระบบสารสนเทศ ต้องได้รับการชี้แจงและทำความเข้าใจเกี่ยวกับนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยสารสนเทศขององค์กร

9.1.4 กำหนดให้ผู้ให้บริการเข้าถึงเฉพาะส่วนที่มีไว้สำหรับการพัฒนาระบบงาน (Develop Environment) เท่านั้น แต่หากมีความจำเป็นต้องเข้าถึงส่วนที่ใช้งานจริง (Production Environment) ก็ต้องมีการควบคุม หรือตรวจสอบการให้บริการของผู้ให้บริการอย่างเข้มงวด เพื่อให้มั่นใจว่าเป็นไปตามขอบเขตที่ได้กำหนดไว้

9.1.5 ดำเนินการเพิกถอนหรือเปลี่ยนสิทธิ์การเข้าถึงระบบงานของผู้ให้บริการที่สิ้นสุดการว่าจ้างหรือเปลี่ยนการจ้างงานโดยทันทีหรือภายในระยะเวลาที่กำหนดไว้

9.1.6 การอนุญาตให้ผู้ให้บริการเข้าสู่ระบบจากระยะไกล ต้องอยู่บนพื้นฐานของความจำเป็นเท่านั้น และไม่เปิดช่องทางติดต่อ (Port) และอุปกรณ์เชื่อมต่อระยะไกลที่ใช้ทิ้งเอาไว้โดยไม่จำเป็น ช่องทางดังกล่าวต้องมีการตัดการเชื่อมต่อเมื่อไม่ได้ใช้งานแล้ว และจะเปิดให้ใช้ได้ต่อเมื่อมีการขออนุมัติจากหัวหน้างานเทคโนโลยีทางการศึกษาก่อนทุกครั้ง

### 9.2 การบริหารการส่งมอบการให้บริการโดยผู้ให้บริการภายนอก

9.2.1 การให้บริการหรือการส่งมอบงานโดยผู้ให้บริการภายนอกจะต้องมีการตกลงทำสัญญารักษาความปลอดภัยหรือข้อตกลงอย่างอื่น ๆ ที่เกี่ยวข้อง การส่งมอบงานหรือบริการใด ๆ โดยผู้ให้บริการภายนอกจะต้องเป็นไปตามสัญญาการให้บริการที่ระบุไว้โดยเคร่งครัด

9.2.2 การปฏิบัติงานของผู้ให้บริการภายนอกที่มาทำการบำรุงรักษาอุปกรณ์ภายในหน่วยงานและต้องเข้าปฏิบัติงานในพื้นที่ควบคุมพิเศษ ผู้ดูแลระบบจะต้องอยู่ในพื้นที่ทุกครั้ง

9.2.3 การเฝ้าระวังและการประเมินผลการดำเนินงานของผู้ให้บริการภายนอก ต้องจัดให้มีการตรวจสอบติดตามและประเมินผลการบริการจากภายนอกเป็นประจำ เพื่อให้มั่นใจได้ว่ามีการปฏิบัติตามข้อตกลงในการรักษาความปลอดภัยของข้อมูลสารสนเทศ และเพื่อให้ได้มีการจัดการกับปัญหาทางด้านความปลอดภัยอย่างเหมาะสม

9.2.4 การบริหารการเปลี่ยนแปลงในบริการจากผู้ให้บริการภายนอก การเปลี่ยนแปลงใด ๆ ที่เกิดจากการดำเนินงานของผู้ให้บริการภายนอก ให้ปฏิบัติตามขั้นตอนในระเบียบปฏิบัติ เรื่อง การบริหารการเปลี่ยนแปลง (รหัสเอกสาร PM-MS-05: Change Management Procedure)

---

# นโยบายการรักษาความมั่นคงปลอดภัยสารสนเทศ

## (10) การบริหารจัดการเหตุการณ์ที่ส่งผลกระทบต่อความมั่นคงปลอดภัยสารสนเทศ (Information Security Incident Management)

10.1 กำหนดให้ผู้รับผิดชอบดำเนินการตามขั้นตอนในระเบียบปฏิบัติ เรื่อง การบริหารอุบัติการณ์สารสนเทศ (รหัสเอกสาร PM-MS-10: Incident Management Procedure)

10.2 การรายงานเหตุการณ์และจุดอ่อนด้านความมั่นคงปลอดภัย ต้องจัดเตรียมช่องทางที่ใช้ในการรายงานเหตุการณ์ด้านความมั่นคงปลอดภัย โดยการประเมินสถานการณ์ และการตัดสินใจดำเนินการตอบสนองต่ออุบัติการณ์ด้านความปลอดภัยสารสนเทศ ต้องเป็นไปตามขั้นตอนในตามระเบียบปฏิบัติ เรื่อง การบริหารอุบัติการณ์สารสนเทศ (รหัสเอกสาร PM-MS-10: Incident Management Procedure)

10.3 ควรมีการรายงานเหตุการณ์ด้านความมั่นคงปลอดภัยและจุดอ่อนด้านความมั่นคงปลอดภัยเผยแพร่ให้บุคลากรในองค์กรทราบ

10.4 การเรียนรู้เหตุการณ์ด้านความปลอดภัยของข้อมูล ควรมีการสรุปและรวบรวมประเภทของเหตุการณ์ และจุดอ่อนด้านความมั่นคงปลอดภัย ตลอดจนผลกระทบอันเกิดจากเหตุการณ์ดังกล่าว เพื่อนำมาใช้ในการปรับปรุงวิธีการรับมือให้มีประสิทธิภาพต่อไป

10.5 การเก็บรวบรวมหลักฐาน ในกรณีที่ต้องมีการเก็บรักษาหลักฐานสนับสนุนอื่น ๆ เช่น อีเมล ไฟร์วอลล์ สิทธิ์การเข้าถึง ระบบตรวจจับการบุกรุก และ log ต่างๆที่เกี่ยวข้อง โดยแนวทางการเก็บรวบรวมหลักฐานต้องสอดคล้องตามระเบียบปฏิบัติ เรื่อง การควบคุมเอกสารข้อมูลและบันทึกคุณภาพ (รหัสเอกสาร PM-AM-01)

---

# นโยบายการรักษาความมั่นคงปลอดภัยสารสนเทศ

## (11) ความมั่นคงปลอดภัยสารสนเทศกับการบริหารความต่อเนื่องทางธุรกิจ

## (Business Continuity Management)

### 11.1 ความต่อเนื่องด้านความมั่นคงปลอดภัยสารสนเทศ

11.1.1 การวางแผนความต่อเนื่องด้านความมั่นคงปลอดภัยสารสนเทศ

ในการจัดทำแผนเตรียมความพร้อมระบบสารสนเทศกรณีฉุกเฉินที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์ได้ ต้องประกอบด้วยรายละเอียดอย่างน้อยดังนี้

1) การวิเคราะห์ความเสี่ยงที่อาจส่งผลกระทบต่อระบบสารสนเทศ
2) ช่องทางการติดต่อผู้เกี่ยวข้องเมื่อเกิดเหตุฉุกเฉิน ทั้งผู้รับผิดชอบภายในองค์กร และผู้ให้บริการภายนอก
3) กระบวนการในการกู้คืนระบบสารสนเทศ
4) ระยะเวลาในการกู้คืนระบบที่สอดคล้องกับเป้าหมายที่กำหนดไว้

11.1.2 การปฏิบัติเพื่อความต่อเนื่องด้านความมั่นคงปลอดภัยสารสนเทศ

11.1.2.1 สร้างความตระหนัก หรือให้ความรู้แก่บุคลากรขององค์กรเกี่ยวกับขั้นตอนการปฏิบัติหรือสิ่งที่ต้องทำเมื่อเกิดเหตุการณ์ฉุกเฉิน

11.1.2.2 จัดการทดสอบเป็นประจำอย่างน้อยปีละ 1 ครั้ง เพื่อให้บุคลากรเข้าใจขั้นตอน และสามารถปฏิบัติงานได้เมื่อเกิดเหตุการณ์ฉุกเฉิน

11.1.3 การทบทวน และการประเมินผลความต่อเนื่องด้านความมั่นคงปลอดภัยสารสนเทศ

11.1.3.1 กำหนดให้มีการทบทวนเพื่อปรับปรุงแผนเตรียมความพร้อมระบบสารสนเทศให้มีความเหมาะสมและสอดคล้องกับการใช้งานตามภารกิจอย่างน้อยปีละ 1 ครั้ง

11.1.3.2 ข้อผิดพลาดหรือปัญหาที่พบในระหว่างการทดสอบจะต้องได้รับการปรับปรุงแก้ไขให้เหมาะสมต่อไป

### 11.2 อุปกรณ์สำรองของกระบวนการในระบบสารสนเทศ

องค์กรต้องมีการจัดหาอุปกรณ์สำรองที่สำคัญที่อาจส่งผลกระทบกับระบบสารสนเทศ อันเนื่องมาจากความล้มเหลวของอุปกรณ์โดยการติดตั้งเพียงหน่วยเดียว รวมทั้งต้องตรวจสอบความพร้อมใช้ของอุปกรณ์เหล่านั้นด้วย เพื่อลดโอกาสของความจำเป็นต้องใช้แผนเตรียมความพร้อมระบบสารสนเทศกรณีฉุกเฉินนั่นเอง

---

# นโยบายการรักษาความมั่นคงปลอดภัยสารสนเทศ

## (12) ความสอดคล้อง

### 12.1 การปฏิบัติตามข้อกำหนดของกฎหมายและเอกสารสัญญาที่เกี่ยวข้อง

12.1.1 เจ้าของระบบสารสนเทศต้องมั่นใจว่าระบบของตนมีการดำเนินการให้เป็นไปตามข้อกำหนดของกฎหมายและข้อกำหนดของหน่วยงานกำกับดูแลทั้งหมด รวมทั้งตามข้อกำหนดในสัญญาที่ทำกับลูกค้า และข้อตกลงในสัญญาการให้บริการ

12.1.2 การปฏิบัติตามข้อกำหนดที่เกี่ยวข้องกับการป้องกันทรัพย์สินทางปัญญา ซอฟต์แวร์ที่ใช้งานในองค์กรจะต้องเป็นซอฟต์แวร์ลิขสิทธิ์และได้รับการอนุมัติให้มีการใช้งานภายในองค์กรเท่านั้น

12.1.3 การป้องกันเอกสารบันทึกขององค์กร บันทึกต่างๆ ที่มีความสำคัญขององค์กรต้องได้รับการป้องกันจากการสูญหาย การทำลาย และการปลอมแปลงที่อาจเกิดขึ้น การจัดเก็บบันทึกต่างๆ จะต้องสอดคล้องและเป็นไปตามข้อกำหนดขององค์กร ข้อกำหนดเชิงกฎหมาย หรือข้อกำหนดที่ระบุไว้ในสัญญาที่ทำไว้กับลูกค้า

12.1.4 การป้องกันใช้งานระบบสารสนเทศใช้โดยมิชอบ การเข้าใช้งานระบบสารสนเทศใดๆ ในองค์กรจะต้องได้รับการอนุมัติอย่างเป็นลายลักษณ์อักษรก่อนที่จะสามารถเข้าใช้งานระบบสารสนเทศได้ ยกเว้นมีความเร่งด่วนที่ต้องดำเนินการ โดยจะต้องแจ้งทางโทรศัพท์ก่อนเพื่อทำการบันทึกและทำเรื่องอนุมัติในภายหลัง

### 12.2 การทบทวนความสอดคล้องทางเทคนิค

12.2.1 กำหนดให้มีการตรวจประเมินระบบเครือข่ายและมาตรการความมั่นคงปลอดภัยของระบบสารสนเทศอย่างน้อยปีละ 1 ครั้ง โดยบุคลากรที่ผ่านการอบรมด้านการตรวจประเมิน เพื่อตรวจสอบความเหมาะสมและประสิทธิภาพของมาตรการควบคุมด้านความมั่นคงปลอดภัยต่างๆ

12.2.2 กำหนดขอบเขตในการตรวจสอบความสอดคล้องในการตั้งค่าระบบ การนำอุปกรณ์ตรวจสอบใด ๆ เข้ามาใช้ในการตรวจสอบระบบ จะต้องได้รับการอนุมัติอย่างเป็นลายลักษณ์อักษรจากเจ้าของระบบก่อนเริ่มดำเนินการ

12.2.3 ผู้ดำเนินการตรวจสอบระบบ จะต้องจัดส่งกำหนดการดำเนินงานให้แก่เจ้าของระบบ เพื่อขอความเห็นชอบก่อนเริ่มดำเนินการ

12.2.4 ผู้ดำเนินการตรวจสอบระบบ ต้องใช้ความระมัดระวังในการดำเนินงาน เพื่อมิให้มีผลกระทบต่อข้อมูลและการให้บริการระบบสารสนเทศที่ได้รับการตรวจสอบ

---