



วิธีปฏิบัติการรักษาความมั่นคงปลอดภัย  
ของระบบเทคโนโลยีสารสนเทศและการสื่อสาร  
มหาวิทยาลัยเทคโนโลยีราชมงคลพระนคร  
2 มิถุนายน 2554

จัดทำโดยกลุ่มเครือข่ายคอมพิวเตอร์และการสื่อสาร  
สำนักวิทยบริการและเทคโนโลยีสารสนเทศ  
มหาวิทยาลัยเทคโนโลยีราชมงคลพระนคร

## วิธีปฏิบัติการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศและการสื่อสาร สำนักวิทยบริการและเทคโนโลยีสารสนเทศ

### หลักการ

สำนักวิทยบริการและเทคโนโลยีสารสนเทศได้มีการประกาศสำนักวิทยบริการและเทคโนโลยีสารสนเทศ เรื่อง นโยบายความมั่นคงปลอดภัยระบบสารสนเทศ มหาวิทยาลัยเทคโนโลยีราชมงคลพระนคร เพื่อให้ระบบเทคโนโลยีสารสนเทศและการสื่อสารของมหาวิทยาลัยเทคโนโลยีราชมงคลพระนคร มีความมั่นคงปลอดภัย ลดความเสี่ยง และปัญหาที่อาจเกิดขึ้นจากการใช้งานที่ไม่ถูกต้อง หรือการคุกคามจากภัยคอมพิวเตอร์

นโยบายการรักษาความมั่นคงปลอดภัยระบบสารสนเทศ มหาวิทยาลัยเทคโนโลยีราชมงคลพระนคร ประกอบด้วยนโยบายแต่ละด้าน ดังนี้ นโยบายความมั่นคงปลอดภัยของเครือข่ายไร้สาย (Wireless Policy), นโยบายความมั่นคงปลอดภัยของไฟร์วอลล์ (Firewall Policy), นโยบายความมั่นคงปลอดภัยของอีเมล (E-mail Policy), นโยบายความมั่นคงปลอดภัยของอินเทอร์เน็ต (Internet Security Policy), นโยบายความมั่นคงปลอดภัยของการควบคุมการเข้าถึงระบบ (Access Control Policy), นโยบายความมั่นคงปลอดภัยของการตรวจจับการบุกรุก (Intrusion Detection System / Intrusion Prevention System Policy : IDS/IPS Policy), นโยบายความมั่นคงปลอดภัยของเครือข่ายและเครื่องคอมพิวเตอร์แม่ข่าย (Network and Server Policy), นโยบายความมั่นคงปลอดภัยของการสำรองข้อมูล (Backup Policy) ซึ่งในนโยบายแต่ละด้านได้กำหนดให้ผู้ดูแลระบบเทคโนโลยีสารสนเทศและการสื่อสาร ดำเนินการบริหารจัดการและกำหนดวิธีการปฏิบัติเพื่อรองรับนโยบายแต่ละด้าน

กลุ่มเครือข่ายคอมพิวเตอร์และการสื่อสาร สำนักวิทยบริการและเทคโนโลยีสารสนเทศ ซึ่งเป็นผู้ดูแลระบบเทคโนโลยีสารสนเทศและการสื่อสาร มหาวิทยาลัยเทคโนโลยีราชมงคลพระนคร จึงจัดทำวิธีการปฏิบัติการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศและการสื่อสารขึ้น เพื่อให้การดำเนินการด้านเทคโนโลยีสารสนเทศและการสื่อสารมีความมั่นคงปลอดภัย และเป็นไปตามกฎหมายและระเบียบปฏิบัติที่เกี่ยวข้อง

อย่างไรก็ตามวิธีปฏิบัติดังกล่าวต้องได้รับความร่วมมือจากผู้ดูแลระบบ และผู้ใช้บริการ ในการปฏิบัติตามอย่างเคร่งครัด จึงหวังเป็นอย่างยิ่งว่าวิธีปฏิบัติการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศและการสื่อสาร มหาวิทยาลัยเทคโนโลยีราชมงคลพระนคร ฉบับนี้ จะเป็นเครื่องมือให้กับผู้ดูแลระบบ และผู้ใช้บริการทุกคน ในการปฏิบัติเพื่อรักษาความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศและการสื่อสาร มหาวิทยาลัยเทคโนโลยีราชมงคลต่อไป

### วัตถุประสงค์

1. เพื่อให้เกิดความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศและการสื่อสาร มหาวิทยาลัยเทคโนโลยีราชมงคลพระนคร
2. เพื่อให้มีวิธีปฏิบัติในการรักษาความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศและการสื่อสาร มหาวิทยาลัยเทคโนโลยีราชมงคลพระนคร ซึ่งสอดคล้องกับกฎหมายและระเบียบปฏิบัติที่เกี่ยวข้อง ให้แก่เจ้าหน้าที่ทุกระดับให้มหาวิทยาลัยเทคโนโลยีราชมงคลพระนคร และบุคคลที่เกี่ยวข้อง ถือปฏิบัติอย่างเคร่งครัด

3. เพื่อสร้างความตระหนักด้านการรักษาความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศและการสื่อสาร ให้แก่เจ้าหน้าที่ทุกระดับในมหาวิทยาลัยเทคโนโลยีราชมงคลพระนคร และบุคคลที่เกี่ยวข้อง
4. เพื่อให้มีการตรวจสอบและประเมินความเสี่ยงในการรักษาความมั่นคงปลอดภัยระบบสารสนเทศและการสื่อสารอย่างสม่ำเสมอ

วิธีปฏิบัติการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศและการสื่อสาร มหาวิทยาลัยเทคโนโลยีราชมงคลพระนคร ประกอบด้วยวิธีการปฏิบัติในด้านต่างๆ ดังนี้

1. วิธีปฏิบัติของผู้ดูแลระบบเทคโนโลยีสารสนเทศและการสื่อสาร
2. วิธีปฏิบัติการกำหนดพื้นที่ใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสาร
3. วิธีปฏิบัติการควบคุมการเข้า-ออกพื้นที่ใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสาร
4. วิธีปฏิบัติการควบคุมสินทรัพย์สารสนเทศและการใช้งานระบบคอมพิวเตอร์
5. วิธีปฏิบัติการบริหารจัดการระบบเครือข่าย
6. วิธีปฏิบัติการควบคุมการเข้าถึงระบบเครือข่าย
7. วิธีปฏิบัติการบริหารจัดการระบบคอมพิวเตอร์ ระบบปฏิบัติการ ระบบสารสนเทศ
8. วิธีปฏิบัติการควบคุมการเข้าถึงระบบคอมพิวเตอร์ ระบบปฏิบัติการ ระบบสารสนเทศ
9. วิธีปฏิบัติการบริหารจัดการเข้าถึงของผู้ใช้บริการ
10. วิธีปฏิบัติการสำรอง และกู้คืนข้อมูล
11. วิธีปฏิบัติการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ
12. วิธีปฏิบัติของผู้ใช้บริการ

## คำนิยาม

คำนิยามที่ใช้ในวิธีปฏิบัตินี้ ประกอบด้วย

- **ส่วนราชการ** หมายถึง ส่วนราชการภายในของมหาวิทยาลัยเทคโนโลยีราชมงคลพระนครที่มีฐานะเป็น สำนัก กอง ศูนย์ หรือหน่วยงานที่เรียกชื่ออย่างอื่นที่มีฐานะเทียบเท่ากอง
- **เทคโนโลยีสารสนเทศและการสื่อสาร** หมายถึง เทคโนโลยีที่เกี่ยวข้องกับข่าวสาร ข้อมูล และการสื่อสาร นับแต่การสร้าง การนำมาวิเคราะห์หรือประมวลผลการรับและส่งข้อมูล การจัดเก็บ และการนำไปใช้งาน ใหม่ เทคโนโลยีเหล่านี้มักจะหมายถึงคอมพิวเตอร์ ซึ่งประกอบด้วยอุปกรณ์ (hardware) ส่วนคำสั่ง (software) และส่วนข้อมูล (data) และระบบการสื่อสารต่างๆ ไม่ว่าจะเป็นโทรศัพท์ ระบบสื่อสารข้อมูล ดาวเทียม หรือเครื่องมือสื่อสารใดๆ ทั้งที่มีสายและไร้สาย
- **ผู้ดูแลระบบเทคโนโลยีสารสนเทศและการสื่อสาร** หมายถึง ผู้ได้รับมอบหมายจากผู้บังคับบัญชาให้มีหน้าที่รับผิดชอบในการบริหารจัดการระบบเทคโนโลยีสารสนเทศและการสื่อสารของส่วนราชการ
- **ผู้ใช้บริการ** หมายถึง ข้าราชการ พนักงานของรัฐ พนักงานราชการ หรือผู้ที่ส่วนราชการ อนุญาตให้ใช้ระบบคอมพิวเตอร์ได้

- **ระบบคอมพิวเตอร์** หมายถึง อุปกรณ์หรือชุดอุปกรณ์ของคอมพิวเตอร์ที่เชื่อมการทำงานเข้าด้วยกันโดยได้มีการกำหนดคำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใด และแนวทางปฏิบัติงานให้อุปกรณ์หรือชุดอุปกรณ์ทำหน้าที่ประมวลผลข้อมูลโดยอัตโนมัติ
- **ระบบเครือข่าย** หมายถึง ระบบที่สามารถใช้ในการติดต่อสื่อสารหรือการส่งข้อมูลและสารสนเทศระหว่างระบบเทคโนโลยีสารสนเทศต่างๆ ของมหาวิทยาลัยได้
- **ระบบสารสนเทศ** หมายถึง กระบวนการจัดเก็บรวบรวมข้อมูลซึ่งทำให้เป็นสารสนเทศ การจัดเก็บและการนำเสนอสารสนเทศให้เป็นปัจจุบัน
- **ไฟร์วอลล์ (Firewall)** หมายถึง เทคโนโลยีป้องกันการบุกรุกจากบุคคลภายนอก เพื่อไม่ให้ผู้ที่มิได้รับอนุญาตเข้ามาใช้ข้อมูลและทรัพยากรในเครือข่าย โดยอาจใช้ทั้งฮาร์ดแวร์และซอฟต์แวร์ในการรักษาความปลอดภัย
- **VPN (Virtual Private Network)** หมายถึง เครือข่ายคอมพิวเตอร์เสมือนที่สร้างขึ้นมาเป็นของส่วนตัว โดยในการรับส่งข้อมูลจริงจะทำโดยการเข้ารหัสเฉพาะแล้วรับ-ส่งผ่านเครือข่ายอินเทอร์เน็ต ทำให้บุคคลอื่นไม่สามารถอ่านได้ และมองไม่เห็นข้อมูลนั้นไปจนถึงปลายทาง
- **WEP (Wired Equivalent Access)** หมายถึง ระบบการเข้ารหัสเพื่อรักษาความปลอดภัยของข้อมูลในเครือข่ายไร้สายโดยอาศัยชุดตัวเลขมาใช้เข้ารหัสข้อมูล ดังนั้นทุกเครื่องในเครือข่ายที่รับ-ส่งข้อมูลถึงกันจึงต้องรู้ค่าชุดตัวเลขนี้
- **WPA (Wi-Fi Protected Access)** หมายถึง ระบบการเข้ารหัสเพื่อรักษาความปลอดภัยของข้อมูลในเครือข่ายไร้สายที่พัฒนาขึ้นมาใหม่ให้มีความปลอดภัยมากกว่าวิธีเดิมอย่าง WEP (Wired Equivalent Access)
- **การพิสูจน์ยืนยันตัวตน (Authentication)** หมายถึง ขั้นตอนการรักษาความปลอดภัยในการเข้าใช้ระบบเป็นขั้นตอนในการพิสูจน์ตัวตนของผู้ใช้บริการระบบทั่วไป แล้วจะเป็นการพิสูจน์โดยใช้ชื่อผู้ใช้บริการ และรหัสผ่าน
- **ลงบันทึกเข้า (Login)** หมายถึง กระบวนการที่ผู้ใช้บริการต้องทำให้เสร็จสิ้นตามเงื่อนไขที่ตั้งไว้เพื่อเข้าใช้งานระบบคอมพิวเตอร์และระบบเครือข่าย ซึ่งปกติแล้วจะอยู่ในรูปแบบของการกรอกชื่อผู้ใช้บริการ และรหัสผ่านให้ถูกต้อง
- **ลงบันทึกออก (Logout)** หมายถึง กระบวนการที่ผู้ใช้บริการทำเพื่อสิ้นสุดการใช้งานระบบคอมพิวเตอร์และระบบเครือข่าย
- **ช่องโหว่ (Vulnerability)** หมายถึง ความอ่อนแอในโปรแกรมคอมพิวเตอร์ซึ่งยอมให้เกิดการกระทำที่ไม่ได้รับอนุญาตได้ โดยเกิดจากข้อบกพร่องจากการออกแบบโปรแกรม ทำให้มีการอาศัยข้อบกพร่องดังกล่าวเพื่อเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต
- **การเข้ารหัส (Encryption)** หมายถึง การนำเอาข้อมูลมาเข้ารหัสเพื่อป้องกันการลักลอบเข้ามาใช้ข้อมูล ผู้ที่สามารถเปิดไฟล์ข้อมูลที่เข้ารหัสไว้จะต้องมีโปรแกรมถอดรหัสเพื่อให้ข้อมูลกลับมาใช้งานได้ตามปกติ
- **เจ้าของข้อมูล** หมายถึง ผู้ได้รับมอบอำนาจจากผู้บังคับขานให้รับผิดชอบข้อมูลของระบบงานโดยเจ้าของข้อมูลเป็นผู้รับผิดชอบข้อมูลนั้นๆ หรือได้รับผลกระทบโดยตรงหากข้อมูลเหล่านั้นเกิดสูญหาย

- **โปรแกรมประสงค์ร้าย (Malware)** หมายถึง โปรแกรมคอมพิวเตอร์ ซุดคำสั่งและ/หรือข้อมูลอิเล็กทรอนิกส์ที่ได้รับการออกแบบขึ้นมาที่มีวัตถุประสงค์เพื่อก่อวินหรือสร้างความเสียหายไม่ว่าโดยตรงหรือโดยอ้อมแก่ระบบคอมพิวเตอร์หรือระบบเครือข่าย เช่น ไวรัสคอมพิวเตอร์ (Computer Virus) หรือสปายแวร์ (Spyware) หรือหนอน (Worm) หรือม้าโทรจัน (Trojan horse) หรือฟิชซิง (Phishing) หรือจดหมายลูกโซ่ (Mass Mailing) เป็นต้น

### วิธีปฏิบัติของผู้ดูแลระบบเทคโนโลยีสารสนเทศและการสื่อสาร

1. กำหนดสิทธิเข้าถึงระบบเทคโนโลยีสารสนเทศและการสื่อสารตามที่ได้รับมอบหมาย โดยกำหนดสิทธิให้ผู้ใช้บริการสามารถใช้บริการได้ตามภารกิจของผู้ใช้บริการ และสามารถเข้าใช้ได้แต่เพียงบริการที่ได้รับอนุญาตให้เข้าถึงเท่านั้น รวมทั้งดำเนินการทบทวนสิทธิการเข้าถึงอย่างสม่ำเสมอ
2. บริหารจัดการการใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารของหน่วยงาน ให้เป็นไปด้วยความเรียบร้อยและมีประสิทธิภาพ หากตรวจพบสิ่งผิดปกติให้รีบดำเนินการแก้ไข รวมทั้งป้องกันและบรรเทาความเสียหายที่อาจจะเกิดขึ้นในทันที ในกรณีที่สิ่งผิดปกติดังกล่าวเกิดขึ้นจากการใช้งานของผู้ใช้บริการที่ไม่เป็นไปตามนโยบายนี้ ให้รีบแจ้งผู้ให้บริการผู้รับผิดชอบให้ยุติการกระทำดังกล่าวในทันที และในกรณีจำเป็นเพื่อป้องกันหรือบรรเทาความเสียหายที่จะเกิดขึ้นแก่หน่วยงานให้ผู้ดูแลระบบพิจารณาระงับการให้บริการของผู้ใช้บริการดังกล่าวทันที
3. ติดตั้งและเปลี่ยนแปลงค่า parameter ต่างๆ ของระบบเทคโนโลยีสารสนเทศและการสื่อสารที่ได้รับมอบหมาย และทบทวนการกำหนดค่า parameter ต่างๆ อย่างน้อยเดือนละครั้ง
4. บริหารจัดการข้อมูลเครื่องคอมพิวเตอร์หรือโปรแกรมคอมพิวเตอร์ ที่เกี่ยวข้องกับการปฏิบัติงานของหน่วยงานสำหรับเครื่องคอมพิวเตอร์แม่ข่าย และอุปกรณ์ต่อพ่วงให้มีความปลอดภัย
5. จัดเก็บข้อมูลจราจรคอมพิวเตอร์ (Log File) ที่เกี่ยวข้องกับการให้บริการของหน่วยงาน เพื่อให้ข้อมูลจราจรทางคอมพิวเตอร์สามารถระบุตัวผู้ใช้นับตั้งแต่เริ่มใช้บริการและต้องเก็บรักษาไว้อย่างครบถ้วน ถูกต้อง ตามพระราชบัญญัติว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550
6. ไม่ใช้อำนาจหน้าที่ของตนในการเข้าถึงข้อมูลของผู้ใช้บริการที่ใช้งานระบบคอมพิวเตอร์โดยไม่มีเหตุผลอันสมควร
7. ไม่เปิดเผยข้อมูลที่ได้มาจากการปฏิบัติหน้าที่ ซึ่งข้อมูลดังกล่าวเป็นข้อมูลที่ไม่เปิดเผยให้บุคคลหนึ่งบุคคลใดทราบ โดยไม่มีเหตุอันสมควร
8. คืนทรัพย์สินของหน่วยงานที่เกี่ยวข้องกับการปฏิบัติหน้าที่ของตนในทันทีที่พ้นจากหน้าที่ และให้ผู้บริหารของหน่วยงาน หรือผู้ที่ได้รับมอบหมาย เพื่อการตรวจสอบการคืนทรัพย์สิน

## วิธีปฏิบัติกาหนดพื้นที่ใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสาร

1. กำหนดพื้นที่ของระบบเทคโนโลยีสารสนเทศและการสื่อสารอย่างเหมาะสม โดยจัดทำเป็นเอกสาร “การกำหนดพื้นที่เพื่อการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ” เพื่อจุดประสงค์ในการเฝ้าระวังควบคุม การรักษาความมั่นคงปลอดภัยจากผู้ที่ไม่ได้รับอนุญาต รวมทั้งป้องกันความเสียหายอื่นๆ ที่อาจเกิดขึ้นได้
2. จัดทำแผนผังแสดงตำแหน่งของที่ใช้งาน โดยกำหนดและแบ่งแยกบริเวณพื้นที่ใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารให้ชัดเจน ซึ่งแบ่งเป็น
  - 1) **พื้นที่ทำงาน** หมายถึง พื้นที่ติดตั้งเครื่องคอมพิวเตอร์ส่วนบุคคล และคอมพิวเตอร์แบบพกพาที่ประจำโต๊ะทำงาน รวมถึงพื้นที่ทำงานของผู้ดูแลระบบ
  - 2) **พื้นที่ติดตั้งและจัดเก็บอุปกรณ์ระบบเทคโนโลยีสารสนเทศและการสื่อสาร** หมายถึง พื้นที่ติดตั้งและจัดเก็บเครื่องคอมพิวเตอร์แม่ข่าย อุปกรณ์เครือข่าย และอุปกรณ์ต่อพ่วง และให้หมายความรวมถึงพื้นที่จัดเก็บข้อมูลคอมพิวเตอร์
  - 3) **พื้นที่ใช้งานระบบเครือข่ายไร้สาย** หมายถึง พื้นที่ในการให้บริการระบบเครือข่ายไร้สาย

## วิธีปฏิบัติการควบคุมการเข้า-ออกพื้นที่ใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสาร

1. ผู้ดูแลระบบจัดทำเอกสาร “ทะเบียนการเข้าออกพื้นที่” ซึ่งระบุรายละเอียดอย่างน้อย ดังนี้ ชื่อ-นามสกุล, ตำแหน่ง, หน่วยงาน, พื้นที่/เครื่องคอมพิวเตอร์และอุปกรณ์ที่ได้รับสิทธิ, รายละเอียดกิจกรรม, ระยะเวลาดำเนินการ และสิทธิที่ได้รับ
2. ผู้ดูแลระบบจัดทำแบบฟอร์มการบันทึกการเข้าออกพื้นที่ใช้งานฯและบันทึกการเข้าออกพื้นที่ใช้งานฯ อย่างสม่ำเสมอ
3. ผู้ดูแลระบบตรวจสอบการบันทึกการเข้าออกพื้นที่ทุกครั้งที่มีการใช้งาน ,รายการอุปกรณ์ให้ถูกต้อง และจะต้องอยู่กับบุคคลที่มาติดต่อตลอดเวลา รวมทั้งตรวจสอบประวัติการเข้าออกพื้นที่ใช้งานระบบเทคโนโลยีสารสนเทศเป็นประจำอย่างน้อย 1 ครั้งต่อเดือน
4. ผู้ดูแลระบบกำหนดสิทธิการเข้าออกพื้นที่ใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสาร ให้เจ้าหน้าที่มีหน้าที่รับผิดชอบเฉพาะ และต้องปฏิบัติงานที่เกี่ยวข้องกับพื้นที่ที่ใช้งานฯ เป็นประจำ ดังนี้
  - 1) ผู้ดูแลระบบควรมีระบบป้องกันและตรวจสอบการเข้าออกพื้นที่อย่างปลอดภัย เช่น การใช้ระบบชีวภาพ(Biometric) หรือ สมาร์ทการ์ด (Smartcard) เป็นต้น
  - 2) ผู้ใช้บริการที่ต้องการเข้าใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสาร จะต้องขออนุญาตและบันทึกการเข้าออกพื้นที่ทุกครั้ง
  - 3) หากมีบุคคลอื่นใดที่ไม่ใช่ผู้บริการ ขอเข้าพื้นที่โดยมิได้ขอสิทธิในการเข้าพื้นที่นั้นไว้เป็นการล่วงหน้า หน่วยงานเจ้าของพื้นที่ ผู้ดูแลระบบต้องตรวจสอบเหตุผลและความจำเป็นก่อนอนุญาต และจดบันทึกการเข้าออกพื้นที่ฯ ไว้เป็นหลักฐาน ทั้งในกรณีที่อนุญาตและไม่อนุญาตให้เข้าพื้นที่

## วิธีปฏิบัติการควบคุมสิทธิ์สารสนเทศและการใช้งานระบบคอมพิวเตอร์

1. ผู้ดูแลระบบต้องจัดทำบัญชีทรัพย์สินด้านเทคโนโลยีสารสนเทศและการสื่อสาร โดยระบุผู้รับผิดชอบในทรัพย์สินอย่างชัดเจน
2. ผู้ดูแลระบบต้องบริหารจัดการทรัพย์สินที่ใช้สำหรับบริการให้บริการระบบคอมพิวเตอร์ และระบบเครือข่ายหลักของหน่วยงาน เพื่อป้องกันไม่ให้เกิดทรัพย์สินเกิดความเสียหายใช้งานไม่ได้ หรือสูญหาย
3. ผู้ดูแลระบบต้องเก็บรักษาอุปกรณ์ของระบบคอมพิวเตอร์และระบบเครือข่าย ในพื้นที่ใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสาร และอนุญาตให้เข้าถึงเฉพาะผู้ดูแลระบบเท่านั้น

## วิธีปฏิบัติการบริหารจัดการระบบเครือข่าย

1. ผู้ดูแลระบบจัดทำแผนผังระบบเครือข่าย ประกอบด้วยรายละเอียดเกี่ยวกับขอบเขตของเครือข่ายภายในและเครือข่ายภายนอกโดยระบุอุปกรณ์ที่ติดตั้งในระบบเครือข่าย, การแบ่งแยกเครือข่ายตามกลุ่มของบริการสารสนเทศ, การกำหนดเส้นทางบนเครือข่าย พร้อมทั้งปรับปรุงให้เป็นปัจจุบันอยู่เสมอ
2. ผู้ดูแลระบบต้องแบ่งแยกเครือข่ายตามกลุ่มขอบบริการสารสนเทศ กลุ่มผู้ใช้บริการ และกลุ่มของระบบสารสนเทศ เช่น โซนภายใน (Internal Zone) โซนภายนอก (External Zone) เป็นต้น เพื่อให้การควบคุม และป้องกันการบุกรุกได้อย่างเป็นระบบ โดยเฉพาะระบบที่ไวต่อการรบกวน มีผลกระทบและมีความสำคัญสูงต่อองค์กร ต้องได้รับการแยกออกจากระบบอื่นๆ และมีการควบคุมสภาพแวดล้อมของตนเองโดยเฉพาะ
3. ผู้ดูแลต้องกำหนดหรือเปลี่ยนแปลงค่า parameter ต่างๆ ของอุปกรณ์ระบบเครือข่ายและอุปกรณ์ต่างๆ และทบทวนการกำหนดค่า parameter ต่างๆ อย่างน้อยเดือนละครั้ง
4. ผู้ดูแลระบบต้องป้องกันพอร์ต โดยควบคุมการเข้าถึงพอร์ตดังกล่าวทั้งการเข้าถึงทางกายภาพและทางเครือข่าย
5. ผู้ดูแลระบบต้องตรวจสอบการโจมตี บุกกรุก การใช้งานในลักษณะที่ผิดปกติ เพื่อความมั่นคงปลอดภัยของระบบเครือข่ายอย่างสม่ำเสมอ โดยบันทึกการใช้งาน และเหตุการณ์ที่น่าสงสัยเกิดขึ้นในระบบเครือข่าย
6. ผู้ดูแลระบบต้องติดตั้งอุปกรณ์หรือโปรแกรมป้องกันการบุกรุก ระหว่างระบบเครือข่ายภายในหน่วยงานกับเครือข่ายภายนอก และระหว่างระบบเครือข่ายไร้สายกับระบบเครือข่ายในหน่วยงาน
7. การติดตั้ง เคลื่อนย้าย หรือทำการใด ๆ กับอุปกรณ์ระบบเครือข่ายต่างๆ ได้แก่ อุปกรณ์จัดเส้นทาง (Router), อุปกรณ์กระจายสัญญาณข้อมูล (Switch), อุปกรณ์ที่เชื่อมต่อกับระบบเครือข่ายหลัก เป็นต้น ต้องได้รับอนุญาตจากผู้ดูแลระบบ
8. ผู้ดูแลระบบที่ให้บริการระบบเครือข่ายไร้สายต้องตรวจสอบความมั่นคงปลอดภัยของระบบเครือข่ายไร้สายอย่างสม่ำเสมอ เพื่อตรวจสอบและบันทึกเหตุการณ์ที่น่าสงสัยเกิดขึ้นในระบบเครือข่ายไร้สาย
9. ผู้ดูแลระบบที่ให้บริการระบบเครือข่ายไร้สายต้องเปลี่ยนค่า SSID (Service Set Identifier) ที่กำหนดเป็นค่าโดยปริยาย (Default) มาจากผู้ผลิตทันทีที่นำ อุปกรณ์กระจายสัญญาณ (Access Point) มาใช้งาน

10. ผู้ดูแลระบบของหน่วยงานที่ให้บริการระบบเครือข่ายไร้สาย ต้องกำหนดค่า WEP (Wired Equivalent Privacy) หรือ WPA (Wi-Fi Protected Access) ในการเข้ารหัสข้อมูลระหว่าง Wireless LAN Client และ อุปกรณ์กระจายสัญญาณ (Access Point) และควรกำหนดค่าให้ไม่แสดงชื่อระบบเครือข่ายไร้สาย
11. ผู้ดูแลระบบต้องกำหนดตำแหน่งการวางอุปกรณ์ Access Point ให้เหมาะสมกับพื้นที่ใช้งาน และควบคุมไม่ให้สัญญาณของอุปกรณ์รั่วไหลออกไปนอกบริเวณที่ใช้งาน เพื่อป้องกันไม่ให้ผู้โจมตีสามารถรับส่งสัญญาณจากภายนอกอาคารหรือบริเวณขอบเขตที่ควบคุมได้
12. ผู้ดูแลระบบ ควรเปลี่ยนค่าชื่อ Login และรหัสผ่านสำหรับการตั้งค่าการทำงานของอุปกรณ์ไร้สาย และผู้ดูแลระบบควรเลือกใช้ชื่อ Login และรหัสผ่านที่มีความคาดเดายากเพื่อป้องกันผู้โจมตีไม่ให้สามารถเดาหรือเจาะรหัสได้โดยง่าย
13. ผู้ดูแลระบบต้องกำหนดค่าใช้ WEP (Wired Equivalent Privacy) หรือ WPA (Wireless Application Protocol) ในการเข้ารหัสหรือข้อมูลระหว่าง Wireless LAN Client และ access Point เพื่อให้ยากต่อการดักจับ
14. ผู้ดูแลระบบต้องบันทึกการทำงานของระบบเครือข่าย บันทึกการปฏิบัติงานของผู้ให้บริการ, บันทึกการบุกรุก, บันทึกการเข้าระบบ, บันทึกการใช้งาน และข้อมูลจราจรทางคอมพิวเตอร์

### วิธีปฏิบัติการควบคุมการเข้าถึงระบบเครือข่าย

1. ผู้ดูแลระบบต้องควบคุมการเข้าถึงระบบเครือข่าย โดยกำหนดขั้นตอนและแบบฟอร์มการใช้งานระบบเครือข่าย ประกอบด้วยรายละเอียดอย่างน้อย ดังนี้ ชื่อผู้ให้บริการ, หมายเลขบัตรประชาชน, หน่วยงาน
2. ผู้ดูแลระบบต้องควบคุมการเข้าถึงระบบเครือข่ายไร้สาย โดยกำหนดขั้นตอนและแบบฟอร์มการใช้งานระบบเครือข่ายไร้สาย ประกอบด้วยรายละเอียดอย่างน้อย ดังนี้ ชื่อผู้ให้บริการ, เหตุผลในการขอใช้, ระยะเวลาในการใช้บริการ
3. ผู้ดูแลระบบต้องควบคุมการจัดเส้นทางบนเครือข่าย ที่เชื่อมต่อกับระบบคอมพิวเตอร์ หรือระบบสารสนเทศที่มีการส่งผ่านหรือไหลเวียนของข้อมูลหรือสารสนเทศ และควบคุมการใช้เส้นทางบนเครือข่ายจากเครื่องคอมพิวเตอร์ลูกข่ายไปยังเครื่องคอมพิวเตอร์แม่ข่าย เพื่อไม่ให้ผู้ให้บริการสามารถใช้เส้นทางอื่นๆ ได้
4. ผู้ดูแลระบบต้องกำหนดสิทธิการเข้าถึงระบบเครือข่าย โดยกำหนดให้ผู้ให้บริการสามารถใช้บริการได้ตามภารกิจของผู้ให้บริการ และได้แต่เพียงบริการที่ได้รับอนุญาตให้เข้าถึงเท่านั้น รวมทั้งดำเนินการทบทวนสิทธิการเข้าถึงอย่างสม่ำเสมอ
5. ผู้ดูแลระบบต้องควบคุมการเข้าถึงระบบเครือข่ายจากระยะไกล (Remote access) โดยกำหนดมาตรการรักษาความมั่นคงปลอดภัย เช่น SSL VPN เป็นต้น และผู้ให้บริการต้องขออนุมัติจากผู้ดูแลระบบตามแบบฟอร์มที่กำหนด ซึ่งแสดงหลักฐานระบุเหตุผลหรือความจำเป็นในการใช้บริการ
6. การอนุญาตให้ผู้ใช้เข้าสู่ระบบจากระยะไกล ต้องอยู่บนพื้นฐานของความจำเป็นเท่านั้น และไม่ควรเปิดพอร์ต (Port) หรือโมเด็ม (Modem) โดยไม่จำเป็น และต้องตัดการเชื่อมต่อเมื่อไม่ได้ใช้งานแล้ว และจะเปิดให้ใช้ได้ต่อเมื่อมีการร้องขอที่จำเป็นเท่านั้น



7. ผู้ใช้บริการระบบเครือข่ายมหาวิทยาลัยเทคโนโลยีราชมงคลพระนคร ต้องพิสูจน์ยืนยันตัวตน (Authentication) ทุกครั้งที่ใช้บริการ

### วิธีการปฏิบัติการบริหารจัดการระบบคอมพิวเตอร์ ระบบปฏิบัติการ ระบบสารสนเทศ

1. ผู้ดูแลระบบต้องบริหารจัดการสิทธิการเข้าระบบ โดยกำหนดชื่อผู้ให้บริการ รหัสผ่าน สิทธิที่ได้รับ เพื่อให้ผู้ให้บริการสามารถใช้บริการได้ตามภารกิจของผู้ให้บริการ และตามสิทธิที่ได้รับอนุญาตให้เข้าถึงเท่านั้น รวมทั้งดำเนินการทบทวนสิทธิการเข้าถึงอย่างสม่ำเสมอ
2. ผู้ดูแลระบบต้องตั้งนาฬิกาของเครื่องคอมพิวเตอร์แม่ข่ายและอุปกรณ์คอมพิวเตอร์ที่ให้บริการทุกชนิดให้ตรงกับเวลาอ้างอิงมาตรฐานระดับชาติ ได้แก่ สถาบันมาตรวิทยาแห่งชาติ, กรมอุตุนิยมวิทยา กองทัพเรือ, ศูนย์ประสานงานการรักษาความปลอดภัยคอมพิวเตอร์ประเทศไทย
3. ผู้ดูแลระบบต้องกำหนดขั้นตอนการตรวจสอบระบบคอมพิวเตอร์ และในกรณีที่พบว่ามีการใช้งานหรือเปลี่ยนแปลงค่าในลักษณะผิดปกติ จะต้องดำเนินการแก้ไขให้ระบบคอมพิวเตอร์สามารถใช้งานได้
4. ผู้ดูแลระบบต้องบันทึกการทำงานของระบบคอมพิวเตอร์อย่างสม่ำเสมอ ได้แก่ บันทึกการปฏิบัติงานของผู้ใช้งาน, บันทึกการทำงานของระบบคอมพิวเตอร์, บันทึกการให้บริการ, บันทึกการทำงานของโปรแกรม, บันทึกข้อมูลจราจรทางคอมพิวเตอร์ เป็นต้น
5. ผู้ใช้บริการที่ต้องการใช้งานพื้นที่เครื่องคอมพิวเตอร์แม่ข่ายที่ให้บริการ Web Server, ชื่อโดเมนย่อย (Sub Domain Name) ของหน่วยงาน, บริการ (Service) ต้องทำหนังสือขออนุญาตต่อผู้อำนวยการสำนักวิทยบริการและเทคโนโลยีสารสนเทศ และรับผิดชอบการจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ในส่วนที่เกี่ยวข้อง และไม่ติดตั้งโปรแกรมใดๆ ที่ส่งผลกระทบต่อการทำงานของระบบและผู้ให้บริการอื่น
6. ผู้ดูแลระบบต้องเปิดบริการ (Service) เท่าที่จำเป็น เช่น บริการ telnet ftp หรือ ping เป็นต้น หากบริการใดที่จำเป็นต้องเปิดบริการมีความเสี่ยงต่อความมั่นคงปลอดภัย ต้องมีมาตรการป้องกันเพิ่มเติมด้วย
7. ผู้ดูแลระบบต้องติดตั้งและปรับปรุงค่า parameter ต่างๆ ให้เป็นปัจจุบัน เพื่ออุดช่องโหว่ต่างๆ ของโปรแกรมระบบ และทดสอบโปรแกรมระบบเกี่ยวกับการรักษาความมั่นคงปลอดภัย และประสิทธิภาพการใช้งานโดยทั่วไป ก่อนติดตั้งและหลังจากการแก้ไขหรือบำรุงรักษา
8. หน่วยงานภายนอก ที่ทำงานให้กับมหาวิทยาลัยเทคโนโลยีราชมงคลพระนครทุกหน่วยงาน ไม่ว่าจะทำงานอยู่ภายในมหาวิทยาลัยเทคโนโลยีราชมงคลพระนครหรือนอกสถานที่ จำเป็นต้องลงนามในสัญญาการไม่เปิดเผยข้อมูลของมหาวิทยาลัยเทคโนโลยีราชมงคลพระนคร โดยสัญญาต้องจัดทำให้เสร็จก่อนให้สิทธิในการเข้าสู่ระบบเทคโนโลยีสารสนเทศและการสื่อสาร

### วิธีปฏิบัติการควบคุมการเข้าถึงระบบคอมพิวเตอร์ ระบบปฏิบัติการ ระบบสารสนเทศ

1. ผู้ดูแลระบบต้องควบคุมการเข้าถึงระบบ โดยกำหนดขั้นตอนและแบบฟอร์มการใช้งานระบบคอมพิวเตอร์ ประกอบด้วยรายละเอียดอย่างน้อย ดังนี้ ชื่อผู้ให้บริการ, เหตุผลในการขอใช้, ระยะเวลาในการใช้บริการ
2. ผู้ดูแลระบบป้องกันการเข้าถึงเครื่องคอมพิวเตอร์แม่ข่าย และอุปกรณ์ต่อพ่วง โดยไม่ได้รับอนุญาต เช่น การใช้กุญแจล็อกที่ตัวเครื่อง, การพิสูจน์ตัวตนยืนยัน เป็นต้น

3. ผู้ดูแลระบบต้องจำกัดระยะเวลาการเชื่อมต่อระบบ โดยตัดการเชื่อมต่อเมื่อไม่ได้งานในช่วงเวลาที่กำหนด
4. เจ้าของข้อมูลหรือเจ้าของระบบต้องกำหนดรายการข้อมูลสำหรับการให้บริการ ประกอบด้วยรายละเอียดอย่างน้อย ดังนี้ ประเภทของข้อมูล, ลำดับความสำคัญ, หรือลำดับชั้นความลับของข้อมูล, ระดับชั้นการเข้าถึง, เวลาที่ได้เข้าถึง, ช่องทางการเข้าถึง เป็นต้น
5. เจ้าของข้อมูลหรือเจ้าของระบบต้องบริหารจัดการการเข้าถึงข้อมูลตามประเภทชั้นความลับสำหรับข้อมูลสำคัญ ในการควบคุมการเข้าถึงข้อมูลแต่ละประเภทชั้นความลับทั้งการเข้าถึงโดยตรงและการเข้าถึงผ่านระบบงาน รวมถึงวิธีการทำลายข้อมูลแต่ละประเภทชั้นความลับ ดังต่อไปนี้
  - 1) ต้องควบคุมการเข้าถึงข้อมูลแต่ละประเภทชั้นความลับทั้งการเข้าถึงโดยตรงและการเข้าถึงผ่านระบบงาน
  - 2) ต้องกำหนดรายชื่อผู้ใช้บริการ และรหัสผ่าน เพื่อใช้ในการตรวจสอบตัวตนจริงของผู้ใช้ข้อมูลในแต่ละชั้นความลับของข้อมูล
  - 3) ควรกำหนดระยะเวลาการใช้งานและระงับการใช้งานทันทีเมื่อพ้นระยะดังกล่าว
  - 4) การรับส่งข้อมูลสำคัญผ่านระบบเครือข่ายสาธารณะ ควรได้รับการเข้ารหัส (Encryption) ที่เป็นมาตรฐานสากล
  - 5) ควรกำหนดการเปลี่ยนรหัสผ่าน ตามระยะเวลาที่กำหนดของระดับความสำคัญของข้อมูล

#### วิธีปฏิบัติการบริหารจัดการการเข้าถึงของผู้ใช้บริการ

1. ผู้ดูแลระบบต้องบริหารจัดการสิทธิการเข้าถึงระบบ โดยกำหนดชื่อผู้ใช้บริการ รหัสผ่าน สิทธิที่ได้รับ เพื่อให้ผู้ใช้บริการสามารถใช้บริการได้ตามภารกิจของผู้ใช้บริการ และตามสิทธิที่ได้รับอนุญาตให้เข้าถึงเท่านั้น รวมทั้งดำเนินการทบทวนสิทธิการเข้าถึงอย่างสม่ำเสมอ
2. ผู้ดูแลระบบต้องตรวจสอบบันทึกการปฏิบัติงานของผู้ใช้บริการอย่างสม่ำเสมอ
3. ผู้ใช้บริการต้องรับทราบสิทธิและหน้าที่เกี่ยวกับการใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสาร และต้องปฏิบัติตามอย่างเคร่งครัด
4. ผู้ดูแลระบบต้องบริหารจัดการสิทธิการใช้งานระบบและรหัสผ่านของผู้ใช้บริการ ดังต่อไปนี้
  - 1) เปลี่ยนแปลงและการยกเลิกรหัสผ่าน เมื่อผู้ใช้บริการระบบลาออก หรือพ้นจากตำแหน่ง หรือยกเลิกการใช้งาน
  - 2) ส่งมอบรหัสผ่านชั่วคราวให้กับผู้ใช้บริการด้วยวิธีการที่ปลอดภัย ควรหลีกเลี่ยงการใช้บุคคลอื่นหรือการส่งจดหมายอิเล็กทรอนิกส์ (e-mail) ที่ไม่มีการป้องกันในการส่งรหัสผ่าน และเมื่อผู้ใช้บริการได้รับรหัสผ่านต้องตอบยืนยันการได้รับรหัสผ่าน
  - 3) กำหนดชื่อผู้ใช้บริการ และรหัสผ่าน ต้องไม่ซ้ำกัน
  - 4) ในกรณีที่มีความจำเป็นต้องให้สิทธิพิเศษกับผู้ใช้บริการที่มีสิทธิสูงสุด ผู้ใช้บริการนั้นจะต้องได้รับความเห็นชอบและอนุมัติจากผู้บังคับบัญชา โดยมีการกำหนดระยะเวลาในการใช้งานและระงับการใช้งานทันทีเมื่อพ้นระยะเวลาดังกล่าวหรือพ้นจากตำแหน่ง และมีการกำหนดสิทธิพิเศษที่ได้รับว่าเข้าถึงได้ถึงระดับใดบ้าง และต้องกำหนดให้รหัสผู้ใช้บริการต่างจากรหัสผู้ไปปกติ

5. เจ้าของข้อมูลหรือเจ้าของระบบต้องบริหารจัดการการเข้าถึงข้อมูลสำคัญตามประเภทชั้นความลับ เพื่อควบคุมป้องกันข้อมูลที่มีความสำคัญ ข้อมูลส่วนบุคคล โดยกำหนดชั้นความลับของข้อมูล, วิธีปฏิบัติในการจัดเก็บข้อมูล และการควบคุมการเข้าถึงข้อมูลแต่ละประเภทชั้นความลับ รวมถึงวิธีการทำลายข้อมูลแต่ละประเภทชั้นความลับ ดังต่อไปนี้
  - 1) กำหนดรายชื่อผู้ใช้บริการ และรหัสผ่าน เพื่อใช้ในการตรวจสอบตัวตนจริงของผู้ใช้ข้อมูลในแต่ละชั้นความลับของข้อมูล
  - 2) กำหนดระยะเวลาการใช้งานและระงับการใช้งานทันทีเมื่อพ้นระยะเวลาดังกล่าว
  - 3) กำหนดการเปลี่ยนรหัสผ่าน ตามระยะเวลาที่กำหนดของระดับความสำคัญของข้อมูล
  - 4) สำรองข้อมูลและลบข้อมูลที่เก็บอยู่ในสื่อบันทึกก่อนนำเครื่องคอมพิวเตอร์ไปให้บุคคลภายนอกใช้งาน หรือการส่งไปตรวจซ่อม

### วิธีปฏิบัติการสำรองและกู้คืนข้อมูล

1. ผู้ดูแลระบบกำหนดเจ้าหน้าที่รับผิดชอบดำเนินการสำรองข้อมูล โดยจัดทำเป็นลายลักษณ์อักษร และให้เจ้าหน้าที่ลงนามรับทราบ
2. ผู้ดูแลระบบกำหนดขั้นตอนปฏิบัติและดำเนินการสำรองข้อมูล และการกู้คืนข้อมูล ที่เหมาะสม และรองรับพระราชบัญญัติ ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 เพื่อให้ระบบอยู่ในสภาพพร้อมใช้งาน และจัดทำแผนเตรียมความพร้อมกรณีเกิดเหตุฉุกเฉิน หรือกรณีมีเหตุการณ์ที่ก่อให้เกิดความเสียหายต่อสารสนเทศ ให้สามารถกู้กลับคืนได้ภายในระยะเวลาที่เหมาะสม
3. ผู้ดูแลระบบต้องทดสอบสภาพพร้อมใช้งานของระบบสารสนเทศ ระบบสำรอง และระบบแผนเตรียมพร้อมกรณีฉุกเฉินตามระยะเวลาที่เพียงพอต่อสภาพความเสี่ยงที่ยอมรับได้ของแต่ละหน่วยงาน
4. ผู้ดูแลระบบต้องจัดทำสำเนาข้อมูลและซอฟต์แวร์เก็บไว้ โดยจัดเรียงตามลำดับความจำเป็นของการสำรองข้อมูลระบบสารสนเทศของหน่วยงานจากเป็นมากไปหาน้อย
5. ผู้ดูแลระบบต้องจัดเก็บข้อมูลที่สำรองนั้นในสื่อเก็บข้อมูล โดยมีการพิมพ์ชื่อบนสื่อเก็บข้อมูลนั้นให้สามารถแสดงถึงระบบซอฟต์แวร์ วันที่ เวลาที่สำรองข้อมูลและผู้รับผิดชอบในการสำรองข้อมูลไว้อย่างชัดเจนข้อมูลที่สำรองควรจัดเก็บไว้ในสถานที่เก็บข้อมูลสำรองซึ่งติดตั้งอยู่ที่สถานที่อื่น และต้องมีการทดสอบสื่อเก็บข้อมูลสำรองอย่างสม่ำเสมอ
6. ผู้ดูแลระบบต้องจัดการกับอุปกรณ์สำหรับสำรองข้อมูลให้ปลอดภัยต่อการเข้าถึงโดยไม่ได้รับอนุญาตและสะดวกต่อการนำมาใช้กู้คืนข้อมูล ในกรณีฉุกเฉินเมื่อข้อมูลที่จัดทำไว้เกิดการเสียหาย

### วิธีปฏิบัติการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ

1. ระบุความเสี่ยงและผลกระทบของความเสี่ยงให้สอดคล้องตามแผนบริหารความเสี่ยงของหน่วยงาน
2. กำหนดวิธีในการประเมินความเสี่ยงและความรุนแรงของผลกระทบที่เกิดจากความเสี่ยงนั้น
3. การประเมินความเสี่ยงให้คำนึงถึงองค์ประกอบดังต่อไปนี้
  - 1) ความรุนแรงของผลกระทบที่เกิดจากความเสี่ยงที่ระบุ

- 2) ภัยคุกคามหรือสิ่งนี้อาจก่อให้เกิดเหตุการณ์ที่ระบุมถึงความเป็นไปได้ที่จะเกิดขึ้น
- 3) จุดอ่อนหรือช่องโหว่ที่อาจถูกใช้ในการก่อให้เกิดเหตุการณ์ที่ระบุ
4. ตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศอาจเกิดขึ้นกับระบบสารสนเทศ อย่างน้อยปีละ 1 ครั้ง โดยผู้ตรวจสอบภายในหน่วยงานของรัฐ หรือโดยผู้ตรวจสอบอิสระด้านความมั่นคงปลอดภัยจากภายนอก เพื่อให้ทราบถึงระดับความเสี่ยงและระดับความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศและการสื่อสารของหน่วยงาน
5. กำหนดหน้าที่และความรับผิดชอบของบุคลากรซึ่งดูแลระบบสารสนเทศ ระบบสำรอง และการจัดทำแผนเตรียมพร้อมกรณีฉุกเฉินในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์
6. ผู้ดูแลระบบจัดทำแผนเตรียมความพร้อมกรณีฉุกเฉินในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์ เพื่อให้สามารถใช้งานสารสนเทศได้ตามปกติอย่างต่อเนื่อง โดยระบุผู้รับผิดชอบและหน้าที่ความรับผิดชอบอย่างชัดเจน โดยต้องปรับปรุงแผนเตรียมความพร้อมกรณีฉุกเฉินดังกล่าวให้สามารถปรับใช้ได้อย่างเหมาะสมและสอดคล้องกับการใช้งานตามภารกิจ
7. ผู้ดูแลระบบทดสอบและปรับปรุงแผนเตรียมความพร้อมฉุกเฉินอยู่เสมอ เพื่อให้แผนมีความทันสมัยและสามารถใช้งานได้หากเกิดเหตุการณ์ขึ้นจริง
8. ผู้ดูแลระบบต้องบันทึกเหตุการณ์ที่เกี่ยวข้องกับการรักษาความปลอดภัยระบบเทคโนโลยีสารสนเทศและการสื่อสารที่เกิดขึ้น โดยพิจารณาถึงประเภท ปริมาณ และหลักฐานสำหรับอ้างอิง เพื่อกรณีที่เหตุการณ์ที่เกิดขึ้นมีความเกี่ยวข้องกับการดำเนินการทางกฎหมาย

### วิธีปฏิบัติของผู้ใช้บริการ

เพื่อให้ผู้ใช้บริการมีความรู้ในการใช้ระบบคอมพิวเตอร์และระบบเครือข่ายอย่างปลอดภัย และปฏิบัติตามอย่างเคร่งครัดซึ่งประกอบด้วย การควบคุมการเข้าถึงระบบคอมพิวเตอร์, การใช้งานบัญชีผู้ใช้บริการ (Account) และรหัสผ่าน (Password), การใช้งานระบบอินเทอร์เน็ต (Internet), การใช้งานจดหมายอิเล็กทรอนิกส์ (e-mail) และการป้องกันจากโปรแกรมประสงค์ร้าย (Malware)

### การควบคุมการเข้าถึงระบบคอมพิวเตอร์ ผู้ใช้บริการควรปฏิบัติดังต่อไปนี้

1. ผู้ใช้บริการต้องปฏิบัติตามประกาศสำนักวิทยบริการและเทคโนโลยีสารสนเทศ เรื่อง นโยบายความมั่นคงปลอดภัยระบบสารสนเทศ มหาวิทยาลัยเทคโนโลยีราชมงคลพระนคร
2. ผู้ใช้บริการต้องทำการพิสูจน์ตัวตนโดยการลงบันทึกเข้า (Login) ทุกครั้งก่อนเข้าใช้บริการสารสนเทศ และต้องรับผิดชอบต่อการกระทำใดๆที่เกิดจากชื่อผู้ใช้บริการ (Username) ไม่ว่าจะการกระทำนั้นจะเกิดจากผู้ใช้บริการหรือไม่ก็ตาม และต้องทำการลงบันทึกออก (Logout) จากระบบ เมื่อเสร็จสิ้นการใช้บริการ หรือเมื่อผู้ใช้บริการไม่อยู่ที่เครื่องคอมพิวเตอร์
3. ห้ามใช้ทรัพยากร ระบบสื่อสารทุกของประเภท รวมถึงอุปกรณ์อื่นใดของมหาวิทยาลัยเทคโนโลยีราชมงคลพระนคร เพื่อขัดขวาง รบกวน โจรกรรมข้อมูลของผู้อื่น

4. ห้ามใช้ทรัพยากร ระบบสื่อสารทุกของประเภท รวมถึงอุปกรณ์อื่นใดของมหาวิทยาลัยเทคโนโลยีราชมงคลพระนคร เพื่อเผยแพร่ ข้อมูล ข้อความ รูปภาพ หรือสิ่งอื่นใดที่ขัดต่อกฎหมายและศีลธรรมอันดี
5. ห้ามใช้ทรัพยากร ระบบสื่อสารทุกของประเภท รวมถึงอุปกรณ์อื่นใดของมหาวิทยาลัยเทคโนโลยีราชมงคลพระนคร เพื่อการปกปิด ปลอมแปลง บิดเบือนข้อมูล ไม่ว่าจะป็นทั้งหมดหรือบางส่วน ที่ทำให้ผู้อื่นเสื่อมเสียชื่อเสียง ถูกดูหมิ่น เกลียดชัง
6. ห้ามใช้ทรัพยากร ระบบสื่อสารทุกของประเภท รวมถึงอุปกรณ์อื่นใดของมหาวิทยาลัยเทคโนโลยีราชมงคลพระนคร เพื่อเผยแพร่ข้อมูลอันเป็นเท็จที่ก่อให้เกิดความเสียหายต่อมหาวิทยาลัยเทคโนโลยีราชมงคลพระนคร หรือความมั่นคงของประเทศ
7. ห้ามติดตั้ง พัฒนาโปรแกรมหรือฮาร์ดแวร์ใดๆ ที่เป็นการทำลายความปลอดภัยของระบบ รวมทั้งการกระทำในลักษณะเป็นการแอบใช้รหัสผ่าน การลักลอบทำสำเนาข้อมูลบุคคลอื่น หรือนำไปใช้เป็นเครื่องมือในการกระทำความผิดตาม พรบ.ว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550
8. ห้ามใช้ทรัพยากร ระบบสื่อสารทุกของประเภทของมหาวิทยาลัยเทคโนโลยีราชมงคลพระนคร เพื่อประโยชน์ทางการค้า หรือนำไปใช้ในกิจกรรมที่มหาวิทยาลัยเทคโนโลยีราชมงคลพระนครไม่ได้กำหนด หรือทำให้เกิดความเสียหายต่อมหาวิทยาลัยเทคโนโลยีราชมงคลพระนคร
9. ห้ามติดตั้งอุปกรณ์ หรือกระทำการใดๆ เพื่อให้สามารถเข้าถึงระบบสารสนเทศของมหาวิทยาลัยเทคโนโลยีราชมงคลพระนคร โดยไม่ได้รับผู้อนุญาตจากผู้มีอำนาจ
10. ผู้ใช้งานต้องไม่นำเครื่องมือ หรืออุปกรณ์อื่นใด เชื่อมเข้าเครือข่ายของมหาวิทยาลัยเทคโนโลยีราชมงคลพระนครเพื่อประกอบธุรกิจส่วนบุคคล

### การใช้งานบัญชีผู้ใช้บริการ และ รหัสผ่าน ผู้ใช้บริการควรปฏิบัติดังต่อไปนี้

1. ผู้ใช้บริการต้องปฏิบัติตามประกาศสำนักวิทยบริการและเทคโนโลยีสารสนเทศ เรื่อง นโยบายความมั่นคงปลอดภัยระบบสารสนเทศ มหาวิทยาลัยเทคโนโลยีราชมงคลพระนคร
2. ผู้ใช้บริการต้องเก็บรักษาหัสผ่าน โดยถือว่าเป็นความลับเฉพาะบุคคล และจะต้องไม่เปิดเผยหรือกระทำการใดให้ผู้อื่นทราบ และไม่บันทึกหรือเก็บรหัสผ่านไว้ในระบบคอมพิวเตอร์โดยไม่ป้องกันการเข้าถึง
3. ผู้ใช้บริการจะต้องลงบันทึกเข้า (Login) โดยใช้บัญชีผู้ใช้บริการของตนเอง และทำการลงบันทึกออก (Logout) ทุกครั้ง เมื่อสิ้นสุดการใช้งานหรือหยุดการใช้งานชั่วคราว
4. ผู้ใช้บริการตั้งการใช้งานโปรแกรมรักษาจอภาพ (Screen Saver) โดยตั้งเวลาประมาณ 5 นาที เพื่อให้ทำการล็อกหน้าจอเมื่อไม่มีการใช้งาน หลังจากนั้นเมื่อต้องการใช้ต้องใส่รหัสผ่าน
5. ผู้ใช้บริการควรกำหนดรหัสผ่าน ดังนี้
  - 1) ผู้ใช้บริการต้องป้องกัน ดูแล รักษา ชื่อผู้ใช้งาน (Username) และรหัสผ่านของตน ห้ามใช้ร่วมกับผู้อื่น รวมทั้งห้ามเผยแพร่ แจกจ่ายรหัสผ่าน
  - 2) รหัสผ่าน ควรมีความยาวไม่น้อยกว่า 8 ตัวอักษร โดยอาจจะมีการผสมกันระหว่างตัวเลข ตัวอักษรที่เป็นตัวพิมพ์เล็กหรือตัวพิมพ์ใหญ่ ตัวอักษรพิเศษและสัญลักษณ์ต่างๆ ด้วย
  - 3) ไม่ควรกำหนดรหัสผ่าน จากชื่อ หรือชื่อสกุลของผู้ใช้บริการ ชื่อบุคคลในครอบครัว บุคคลที่มีความสัมพันธ์กับตนหรือคำศัพท์ที่ใช้ในพจนานุกรม หรือหมายเลขโทรศัพท์

- 4) ควรทำการเปลี่ยนรหัสผ่าน เพื่อใช้งานเครื่องคอมพิวเตอร์ของหน่วยงานอย่างน้อยทุก 6 เดือน หรือเปลี่ยนรหัสผ่าน ทุกครั้งที่มีสัญญาณบอกเหตุว่าอาจรั่วไหล
6. ผู้ใช้บริการต้องมีส่วนร่วมในการดูแลรักษาข้อมูลของมหาวิทยาลัยเทคโนโลยีราชมงคลพระนคร หากเกิดการสูญหาย มีการนำไปใช้ในทางที่ผิด หรือมีการเผยแพร่โดยไม่ได้รับอนุญาต ผู้ใช้บริการต้องมีส่วนร่วมในการรับผิดชอบนั้นด้วย
7. มหาวิทยาลัยเทคโนโลยีราชมงคลพระนครมีสิทธิที่จะระงับหรือบล็อกการใช้งานของเครื่องคอมพิวเตอร์ลูกข่ายที่มีพฤติกรรมการใช้งานที่ผิดนโยบาย หรือเกิดจากการทำงานของโปรแกรมที่มีความเสี่ยงต่อการปลอดภัย จนกว่าจะได้รับการแก้ไข
8. หากเกิดปัญหาในการเข้าใช้งานระบบสารสนเทศใดๆ ก็ดี ผู้ใช้บริการต้องแจ้งให้ผู้ดูแลทราบทันที

### การใช้งานระบบอินเทอร์เน็ต (Internet) ผู้ใช้บริการควรปฏิบัติดังต่อไปนี้

1. ผู้ใช้บริการต้องปฏิบัติตามประกาศสำนักวิทยบริการและเทคโนโลยีสารสนเทศ เรื่อง นโยบายความมั่นคงปลอดภัยระบบสารสนเทศ มหาวิทยาลัยเทคโนโลยีราชมงคลพระนคร
2. ผู้ใช้บริการต้องเชื่อมต่อระบบคอมพิวเตอร์เพื่อการใช้งานระบบอินเทอร์เน็ต ผ่านระบบรักษาความปลอดภัยที่หน่วยงานจัดสรรไว้เท่านั้น และห้ามผู้บริการทำการเชื่อมต่อระบบคอมพิวเตอร์ผ่านช่องทางอื่น ยกเว้นว่ามีเหตุผลความจำเป็นและทำการขออนุญาตจากผู้อำนวยการกองแผนงานเป็นลายลักษณ์อักษรแล้ว
3. ผู้ใช้บริการต้องระมัดระวังการดาวน์โหลดโปรแกรมใช้งานจากระบบอินเทอร์เน็ต ซึ่งรวมถึงการดาวน์โหลดการปรับปรุง (Update) โปรแกรมต่างๆ ต้องเป็นไปโดยไม่ละเมิดลิขสิทธิ์หรือทรัพย์สินทางปัญญา
4. หลังจากใช้งานระบบอินเทอร์เน็ต (Internet) เสร็จแล้ว ให้ผู้บริการทำการลงบันทึกออก (Logout) เพื่อป้องกันการเข้าใช้งานโดยบุคคลอื่นๆ

### การใช้งานจดหมายอิเล็กทรอนิกส์ (e-mail) ผู้ใช้บริการควรปฏิบัติดังต่อไปนี้

1. ผู้ใช้บริการต้องปฏิบัติตามประกาศสำนักวิทยบริการและเทคโนโลยีสารสนเทศ เรื่อง นโยบายความมั่นคงปลอดภัยระบบสารสนเทศ มหาวิทยาลัยเทคโนโลยีราชมงคลพระนคร
2. ผู้ใช้บริการต้องใช้จดหมายอิเล็กทรอนิกส์กลางของมหาวิทยาลัยเทคโนโลยีราชมงคลพระนครในการติดต่อเรื่องที่เป็นราชการเท่านั้น
3. ผู้ใช้บริการที่ต้องการขอลงทะเบียนบัญชีผู้บริการจดหมายอิเล็กทรอนิกส์ (e-mail) ต้องทำการกรอกข้อมูลคำขอเข้าใช้บริการจดหมายอิเล็กทรอนิกส์ (e-mail) ของหน่วยงาน ยื่นคำขอกับเจ้าหน้าที่เพื่อดำเนินการกำหนดสิทธิบัญชีผู้บริการรายใหม่และรหัสผ่าน
4. ผู้บริการที่ได้รับรหัสผ่านครั้งแรกในการผ่านเข้าระบบจดหมายอิเล็กทรอนิกส์ (e-mail) และเมื่อมีการเข้าสู่ระบบในครั้งแรกนั้นจะต้องเปลี่ยนรหัสผ่านโดยทันที
5. หลังจากการใช้งานระบบจดหมายอิเล็กทรอนิกส์ (e-mail) เสร็จสิ้นผู้บริการควรทำการลงบันทึกออก (Logout) ทุกครั้ง เพื่อป้องกันบุคคลอื่นเข้าใช้งานจดหมายอิเล็กทรอนิกส์ (e-mail)

6. ในกรณีที่ต้องการส่งข้อมูลที่เป็นความลับ ผู้ใช้บริการไม่ควรระบุความสำคัญของข้อมูลลงในหัวข้อจดหมายอิเล็กทรอนิกส์ (e-mail)

### การป้องกันจากโปรแกรมประสงค์ร้าย (Malware) ผู้ใช้บริการควรปฏิบัติดังต่อไปนี้

1. ผู้ใช้บริการต้องปฏิบัติตามประกาศสำนักวิทยบริการและเทคโนโลยีสารสนเทศ เรื่อง นโยบายความมั่นคงปลอดภัยระบบสารสนเทศ มหาวิทยาลัยเทคโนโลยีราชมงคลพระนคร
2. ผู้ใช้บริการต้องติดตั้งและใช้งานโปรแกรมคอมพิวเตอร์สำหรับป้องกันและกำจัดโปรแกรมประสงค์ร้าย (Malware) รวมทั้งทำการปรับปรุงให้ทันสมัยอยู่เสมอ
3. ผู้ใช้บริการควรทำการปรับปรุงระบบปฏิบัติการ เว็บเบราว์เซอร์ และโปรแกรมการใช้งานต่างๆ อย่างสม่ำเสมอ เพื่อปิดช่องโหว่ (Vulnerability) ที่เกิดขึ้นจากซอฟต์แวร์และป้องกันการโจมตีจากภัยคุกคาม
4. ห้ามมิให้ผู้บริการทำการปิดหรือยกเลิกระบบป้องกันโปรแกรมประสงค์ร้ายที่ติดตั้งอยู่บนเครื่องคอมพิวเตอร์ โดยมิได้รับอนุญาตจากผู้ดูแลระบบ
5. ผู้บริการที่มีเครื่องคอมพิวเตอร์ที่ติดตั้งโปรแกรมประสงค์ร้าย ต้องไม่เชื่อมต่อคอมพิวเตอร์ดังกล่าวเข้ากับระบบเครือข่าย เพื่อป้องกันการแพร่กระจายของโปรแกรมประสงค์ร้ายไปยังเครื่องคอมพิวเตอร์อื่นๆ
6. ผู้บริการควรตรวจสอบสื่อบันทึกพกพาก่อนการใช้งาน เช่น Floppy Disk, Thumb Drive และ Data Storage เพื่อป้องกันและกำจัดโปรแกรมประสงค์ร้าย
7. มหาวิทยาลัยเทคโนโลยีราชมงคลพระนคร ได้ให้ความสำคัญต่อเรื่องทรัพย์สินทางปัญญา ดังนั้นซอฟต์แวร์ที่อนุญาตให้ใช้งาน หรือมหาวิทยาลัยมีลิขสิทธิ์ ผู้ใช้งานสามารถใช้ได้ตามความจำเป็น และห้ามผู้ใช้งานติดตั้ง หรือใช้งานซอฟต์แวร์อื่นใดที่ไม่มีลิขสิทธิ์ หากมีการตรวจสอบพบความผิดละเมิดลิขสิทธิ์ ถือว่าเป็นความผิดส่วนบุคคล ผู้ใช้งานจะต้องรับผิดชอบแต่เพียงผู้เดียว