

## แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ งานศูนย์ข้อมูลสารสนเทศ วิทยาลัยเทคนิคน่าน

### 1. หลักการและเหตุผล

ตามพระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ.๒๕๔๙ กำหนดให้หน่วยงานของรัฐต้องจัดทำแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ เพื่อให้ระบบเทคโนโลยีสารสนเทศของ วิทยาลัยเทคนิคมหาสารคาม เป็นไปอย่างเหมาะสม มีประสิทธิภาพ มีความมั่นคงปลอดภัยและสามารถดำเนินงานได้อย่างต่อเนื่องรวมทั้งป้องกันปัญหาที่อาจจะเกิดขึ้นจากการใช้งานระบบเทคโนโลยีสารสนเทศในลักษณะที่ไม่ถูกต้องและการถูกคุกคามจากภัยต่างๆ งานศูนย์ข้อมูลสารสนเทศ จึงเห็นสมควรกำหนดนโยบายการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ โดยกำหนดให้มีมาตรฐาน (Standard) แนวปฏิบัติ (Guideline) ขั้นตอนปฏิบัติ (Procedure) ให้ครอบคลุมด้านการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศและป้องกันภัยคุกคามต่างๆ

### 2. วัตถุประสงค์

2.1 การจัดทำนโยบายการรักษาความมั่นคงปลอดภัยด้านสารสนเทศเพื่อให้เกิดความเชื่อมั่นและมีความมั่นคงปลอดภัยในการใช้งานระบบเทคโนโลยีสารสนเทศและเครือข่ายคอมพิวเตอร์ขององค์กร ทำให้ดำเนินงานได้อย่างมีประสิทธิภาพและประสิทธิผล

2.2 กำหนดขอบเขตของการบริหารจัดการความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศอ้างอิงตามมาตรฐาน ISO/IEC 27001 และมีการปรับปรุงอย่างต่อเนื่อง

2.3 นโยบายนี้จะต้องทำการเผยแพร่ให้เจ้าหน้าที่ทุกระดับในองค์กรได้รับทราบและเจ้าหน้าที่ทุกคนจะต้องลงนามยอมรับและปฏิบัติตามนโยบายนี้อย่างเคร่งครัด

2.4 เพื่อกำหนดมาตรฐาน แนวทางปฏิบัติและวิธีปฏิบัติ ให้ผู้บริหาร เจ้าหน้าที่ ผู้ดูแลระบบและบุคคลภายนอกที่ปฏิบัติงานให้กับองค์กร ตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัยในการใช้ระบบเทคโนโลยีสารสนเทศขององค์กรในการดำเนินงานและปฏิบัติตามอย่างเคร่งครัด

2.5 นโยบายนี้ต้องมีการดำเนินการตรวจสอบและประเมินนโยบายตามระยะเวลาอย่างน้อย 1 ครั้งต่อปี

### 3. นโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

3.1 ส่งเสริมและสนับสนุนการรักษาความมั่นคงปลอดภัยด้านสารสนเทศให้ตอบสนองต่อ พันธกิจและนโยบายขององค์กร

3.2 มุ่งกำหนดแนวปฏิบัติ แนวทางแก้ไข หรือบทลงโทษตามความเหมาะสมหากมีการละเมิดหรือฝ่าฝืนแนวนโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ รวมทั้งติดตามและตรวจสอบการดำเนินงานอย่างสม่ำเสมอ เพื่อให้เป็นไปตามกฎหมายและระเบียบปฏิบัติที่เกี่ยวข้อง

3.3 เน้นกำกับดูแลการดำเนินงานเพื่อบริหารจัดการให้ระบบเทคโนโลยีสารสนเทศมีความถูกต้อง สมบูรณ์ และพร้อมใช้งานอยู่เสมอ

3.4 เผยแพร่ความรู้ ความเข้าใจเพื่อสร้างความตระหนักให้บุคลากรที่เกี่ยวข้องทั้งของหน่วยงานเอง และของหน่วยงานที่เกี่ยวข้อง ตลอดจนส่งเสริมให้มีการศึกษาอย่างต่อเนื่อง

3.5 ติดตาม ตรวจสอบการดำเนินงาน และปรับปรุงแผนนโยบายและแนวปฏิบัติในการรักษาความ มั่นคงปลอดภัยด้านสารสนเทศให้สอดคล้องตามการเปลี่ยนแปลงของเทคโนโลยี

#### 4. องค์ประกอบของนโยบาย

4.1 คำนินยาม

4.2 การรักษาความมั่นคงปลอดภัยทางกายภาพและสิ่งแวดล้อม

4.3 การรักษาความมั่นคงปลอดภัยของการควบคุมการเข้าถึงระบบ

4.4 การรักษาความมั่นคงปลอดภัยของเครือข่ายและเครื่องคอมพิวเตอร์แม่ข่าย

4.5 การรักษาความมั่นคงปลอดภัยของเครือข่ายไร้สาย

4.6 การรักษาความมั่นคงปลอดภัยของไฟร์วอลล์

4.7 การรักษาความมั่นคงปลอดภัยของอีเมลล์

4.8 การรักษาความมั่นคงปลอดภัยของอินเทอร์เน็ต

4.9 การรักษาความมั่นคงปลอดภัยของการตรวจจับการบุกรุก

4.10 ความมั่นคงปลอดภัยของการสำรองข้อมูล

4.11 การสร้างความตระหนักในเรื่องการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

นโยบายการรักษาความมั่นคงปลอดภัยด้านสารสนเทศขององค์กร แต่ละส่วนที่กล่าวข้างต้น จะประกอบด้วย วัตถุประสงค์ แนวทางปฏิบัติ (Guideline) และขั้นตอนวิธีการปฏิบัติ (Procedure) ในการ รักษาความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศขององค์กร เพื่อที่จะทำให้องค์กรมีมาตรการในการ รักษาความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศอยู่ในระดับที่ปลอดภัย ช่วยลดความเสียหายต่อการ ดำเนินงาน ทรัพย์สิน บุคลากร ขององค์กร ทำให้สามารถดำเนินงานได้อย่างมั่นคงปลอดภัย

นโยบายการใช้งานระบบเทคโนโลยีสารสนเทศขององค์กรนี้ จัดเป็นมาตรฐานด้านความปลอดภัย ในการใช้งานระบบเทคโนโลยีสารสนเทศขององค์กร ซึ่งเจ้าหน้าที่ขององค์กรและหน่วยงานภายนอกจะต้อง ปฏิบัติตามอย่างเคร่งครัด