ประกาศมหาวิทยาลัยเทคโนโลยีราชมงคลธัญบุรี

เรื่อง นโยบายรักษาความปลอดภัยด้านเทคโนโลยีสารสนเทศ

เนื่องจากในปัจจุบันมหาวิทยาลัยเทคโนโลยีราชมงคลธัญบุรีใช้เทคโนโลยีสารสนเทศเป็นเครื่องมือในการดำเนินการและกิจกรรมต่างๆอย่างแพร่หลาย ซึ่งการใช้เทคโนโลยีสารสนเทศดังกล่าวอาจก่อให้เกิดความเสี่ยงในการดำเนินงานของมหาวิทยาลัยฯหลายประการ โดยความเสี่ยงที่มหาวิทยาลัยฯให้ความสำคัญ ได้แก่

1. ความเสี่ยงเกี่ยวกับการเข้าถึงข้อมูลและระบบคอมพิวเตอร์โดยบุคคลที่ไม่มีอำนาจหน้าที่เกี่ยวข้อง(Confidentiality Risk)
2. ความเสี่ยงเกี่ยวกับการที่บุคคลที่มีอำนาจหน้าที่ไม่สามารถเข้าถึงข้อมูลในระบบคอมพิวเตอร์ในส่วนที่เกี่ยวข้องกับงานที่รับผิดชอบ และการที่ไม่สามารถใช้ข้อมูลหรือระบบคอมพิวเตอร์ได้อย่างต่อเนื่องหรือในเวลาที่ต้องการ(Availability Risk)
3. ความเสี่ยงเกี่ยวกับความถูกต้องครบถ้วนของข้อมูลและการป้องกันการแก้ไขข้อมูลให้เปลี่ยนไปจากต้นฉบับ (Integrity Risk)

ซึ่งความเสี่ยงตามที่กล่าวมาข้างต้นอาจก่อให้เกิดความเสียหายต่อการดำเนินกิจกรรมตามภารกิจของมหาวิทยาลัยฯได้ ดังนั้น เพื่อเป็นการป้องกันความเสี่ยงเกี่ยวกับการใช้เทคโนโลยีสารสนเทศมหาวิทยาลัยฯจึงได้กำหนดนโยบายรักษาความปลอดภัยด้านเทคโนโลยีสารสนเทศ ไว้ดังนี้

ข้อ 1 ในประกาศนี้

"หน่วยงาน" หมายความว่า หน่วยงานต่างๆ ภายในและภายนอกมหาวิทยาลัยเทคโนโลยีราชมงคลธัญบุรี ที่มีการเชื่อมต่อ และใช้เครือข่ายเทคโนโลยีสารเทศของมหาวิทยาลัยฯ

ข้อ 2 หน่วยงานต้องมีการดำเนินการตามประกาศและบังคับใช้ระเบียบปฏิบัติเกี่ยวกับ

2.1 แนวทางการควบคุมการปฏิบัติงานและการรักษาความปลอดภัยด้านเทคโนโลยีสารสนเทศ

2.2 ข้อบังคับสำหรับผู้ดูแลระบบเครือข่าย

2.3 ข้อบังคับสำหรับผู้เข้าใช้งานระบบเครือข่าย

ทั้งนี้ให้เป็นไปตามเงื่อนไขและลักษณะของการดำเนินงานที่ต้องมีการกำหนดระดับของการควบคุม ตามระดับของความสำคัญและความเสี่ยงของแต่ละหน่วยงาน ตามที่มหาวิทยาลัยฯ หรือคณะกรรมการที่มหาวิทยาลัยฯ มอบหมายกำหนดขึ้น

ข้อ 3 มหาวิทยาลัยฯจะจัดให้มีการประเมินและรายงานความเสี่ยง การตรวจสอบการปฏิบัติงานด้านเทคโนโลยีสารสนเทศ ภายใต้ข้อกำหนดของทางมหาวิทยาลัยฯตามระดับความเสี่ยงของกิจกรรมที่ดำเนินการในแต่ละหน่วยงาน โดยคณะกรรมการหรือหน่วยงานที่มหาวิทยาลัยฯ มอบหมาย

ข้อ 4 หน่วยงานต้องจัดให้มีระบบการสอบยันการปฏิบัติงานระหว่างบุคลากรในหน่วยงาน โดยอย่างน้อยต้องไม่มอบหมายให้บุคลากรคนหนึ่งคนใดรับผิดชอบการปฏิบัติงานตลอดกระบวนการในลักษณะที่อาจเป็นช่องทางให้มีการแก้ไขหรือเปลี่ยนแปลงข้อมูลหรือการทำงานของระบบคอมพิวเตอร์โดยมิชอบ

ข้อ 5 หน่วยงานที่มีศูนย์คอมพิวเตอร์ต้องจัดให้มีระบบการรักษาความปลอดภัยทางกายภาพที่เพียงพอแก่การป้องกันมิให้บุคคลที่ไม่มีอำนาจหน้าที่เกี่ยวข้องได้เข้าถึงอุปกรณ์คอมพิวเตอร์ที่สำคัญซึ่งจัดเก็บอยู่ในศูนย์คอมพิวเตอร์ และต้องจัดให้มีระบบป้องกันความเสียหายจากสภาวะแวดล้อมหรือภัยพิบัติต่างๆ ให้แก่อุปกรณ์คอมพิวเตอร์ที่สำคัญภายในศูนย์คอมพิวเตอร์ด้วย

ข้อ 6 หน่วยงานต้องจัดให้มีระบบการรักษาความปลอดภัยของข้อมูล ระบบคอมพิวเตอร์และระบบเครือข่าย ที่เพียงพอแก่การป้องกันมิให้บุคคลที่ไม่มีอำนาจหน้าที่เกี่ยวข้องได้เข้าถึงล่วงรู้ใช้ประโยชน์ หรือแก้ไขเปลี่ยนแปลงข้อมูลหรือระบบดังกล่าวได้

ข้อ 7 หน่วยงานต้องจัดให้มีมาตรการควบคุมที่เพียงพอเพื่อให้ระบบงานคอมพิวเตอร์ (Application Software) ที่ได้รับการพัฒนาหรือแก้ไขเปลี่ยนแปลงมีการประมวลผลที่ถูกต้องครบถ้วนและเป็นไปตามความต้องการของผู้ใช้งาน รวมทั้งต้องสื่อสารการพัฒนาหรือการเปลี่ยนแปลง ให้ผู้ที่เกี่ยวข้องได้รับทราบอย่างทั่วถึงเพื่อให้สามารถใช้งานได้อย่างถูกต้อง

ข้อ 8 หน่วยงานต้องจัดให้มีการสำรองข้อมูลและระบบคอมพิวเตอร์ตลอดจนแผนสำรองกรณีฉุกเฉิน เพื่อให้สามารถรองรับการดำเนินงานได้อย่างต่อเนื่อง มีประสิทธิภาพและทันต่อเหตุการณ์

ข้อ 9 หน่วยงานต้องจัดให้มีมาตรการในการควบคุมการปฏิบัติงานประจำของเจ้าหน้าที่และผู้ดูแลระบบงานด้านคอมพิวเตอร์ อบรมให้ความรู้กับผู้ใช้งานระบบเครือข่าย อย่างเพียงพอ เพื่อให้สามารถใช้งานระบบคอมพิวเตอร์และการประมวลผลข้อมูลสามารถทำงานได้อย่างต่อเนื่องและถูกต้องครบถ้วน ตลอดจนการประสานงานกับองค์กรต่างๆที่เกี่ยวข้อง ทั้งภาครัฐและเอกชนในการแลกเปลี่ยนข้อมูลข่าวสารในการป้องกันระบบงานและแก้ไขข้อขัดข้อง

ข้อ 10 ในกรณีที่หน่วยงานใช้บริการงานเทคโนโลยีสารสนเทศของผู้ให้บริการที่เป็นบุคคลภายนอก ต้องจัดให้มีหลักเกณฑ์ในการคัดเลือกและพิจารณาความเหมาะสมของผู้ให้บริการ รวมทั้งต้องควบคุมและตรวจสอบการปฏิบัติงานของผู้ให้บริการอย่างเข้มงวด เพื่อให้มั่นใจว่าผู้ให้บริการสามารถปฏิบัติงานตามข้อกำหนดในประกาศนี้ได้

ข้อ 11 หากมีผู้ละเมิดและกระทำผิดต่อ ระเบียบข้อบังคับต่างๆ ที่ทางมหาวิทยาลัยฯกำหนดขึ้น ตลอดจนการกระทำผิดต่อกฎหมาย และศีลธรรมอันดี จะต้องถูกพิจารณาดำเนินการลงโทษตามบทบัญญัติที่กฎหมายและข้อบังคับต่างๆกำหนดขึ้น

ข้อ 12 เพื่อให้หน่วยงานสามารถปฏิบัติตามข้อกำหนดในประกาศนี้อย่างมีประสิทธิภาพ และมีมาตรฐานเป็นที่ยอมรับสอดคล้องกับการดำเนินงานในส่วนต่างๆของมหาวิทยาลัยฯ รวมไปถึงภาครัฐบาลและองค์กรอื่นๆ ให้หน่วยงานปฏิบัติตามแนวทางปฏิบัติ (Guideline) เกี่ยวกับการควบคุมการปฏิบัติงานและการรักษาความปลอดภัยด้านเทคโนโลยีสารสนเทศ ตามประกาศของมหาวิทยาลัยฯ กำหนด ให้มีคณะกรรมการกำกับดูแลตามประกาศนโยบาย

ในกรณีที่หน่วยงานดำเนินการในแนวทางปฏิบัติอื่นที่แตกต่างจากแนวทางที่มหาวิทยาลัยฯ กำหนด มหาวิทยาลัยฯ จะพิจารณาว่าหน่วยงานได้ปฏิบัติให้เป็นไปตามข้อกำหนดในประกาศนี้ต่อเมื่อหน่วยงานสามารถแสดงได้ว่าแนวทางอื่นนั้นสามารถป้องกันความเสี่ยงด้านเทคโนโลยีสารสนเทศได้ และมีประสิทธิภาพเพียงพอ ตลอดจนอยู่ในมาตรฐานที่ยอมรับได้สำหรับการควบคุมการปฏิบัติงานและการรักษาความปลอดภัยด้านเทคโนโลยีสารสนเทศ

ประกาศ ณ วันที่ เดือน สิงหาคม พ.ศ. 2549

(ผู้ช่วยศาสตราจารย์นำยุทธ สงค์ธนาพิทักษ์)
อธิการบดีมหาวิทยาลัยเทคโนโลยีราชมงคลธัญบุรี