ประกาศมหาวิทยาลัยกาฬสินธุ์
เรื่อง นโยบายและข้อปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ
มหาวิทยาลัยกาฬสินธุ์ พ.ศ. ๒๕๖๑

มหาวิทยาลัยกาฬสินธุ์เป็นมหาวิทยาลัยที่มุ่งเน้นการผลิตบัณฑิตวิชาชีพ เทคโนโลยี นวัตกรรม และบูรณาการ ภูมิปัญญาท้องถิ่น เพื่อพัฒนาชุมชน สังคมในภูมิภาคลุ่มแม่น้ำโขงและสากล โดยมีการบริหารงานที่โปร่งใส สอดคล้องกับนโยบายของรัฐบาล ให้ก้าวเข้าสู่ไทยแลนด์ ๔.๐ ซึ่งปัจจุบันมหาวิทยาลัยฯ มีนโยบายในการนำระบบสารสนเทศเข้ามาบริหารจัดการ การศึกษา จึงเป็นการสมควรกำหนดแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของมหาวิทยาลัยกาฬสินธุ์ ให้สอดคล้องกับพระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ. ๒๕๕๓ ซึ่งกำหนดให้หน่วยงานของรัฐจัดทำแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศเพื่อให้การดำเนินการใดๆ ด้วยวิธีการทางอิเล็กทรอนิกส์กับหน่วยงานของรัฐหรือโดยหน่วยงานของรัฐมีความมั่นคงปลอดภัยและเชื่อถือได้

อาศัยอำนาจตามความในมาตรา ๓๑ แห่งพระราชบัญญัติมหาวิทยาลัยกาฬสินธุ์ พ.ศ. ๒๕๕๘ จึงให้ออกประกาศ เรื่อง นโยบายและข้อปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ มหาวิทยาลัยกาฬสินธุ์ พ.ศ. ๒๕๖๑ ไว้ดังต่อไปนี้

ข้อ ๑ ประกาศนี้เรียกว่า “ ประกาศมหาวิทยาลัยกาฬสินธุ์ เรื่อง นโยบายและข้อปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ มหาวิทยาลัยกาฬสินธุ์ พ.ศ.๒๕๖๑”

ข้อ ๒ ประกาศนี้มีผลใช้บังคับตั้งแต่วันถัดจากวันประกาศเป็นต้นไป

ข้อ ๓ นโยบายและข้อปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ตามประกาศนี้ประกอบด้วยเนื้อหา ๒ ส่วน ดังนี้

๓.๑ นโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศมีเนื้อหาครอบคลุมตามข้อ ๔

๓.๒ ข้อปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ มีเนื้อหาครอบคลุมตามข้อ ๕ ถึง ข้อ ๑๒

ข้อ ๔ นโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ตามประกาศนี้ประกอบด้วยเนื้อหา ๒ ส่วน ดังนี้

๔.๑ ส่วนที่ว่าด้วยการจัดทำนโยบาย

๑. ผู้บริหาร เจ้าหน้าที่ผู้ปฏิบัติงานด้านคอมพิวเตอร์และผู้ใช้งานได้มีส่วนร่วมในการทำนโยบาย

๒. นโยบายได้จัดทำเป็นลายลักษณ์อักษร โดยมีการประกาศให้ผู้ใช้งานได้รับทราบและสามารถเข้าถึงได้ โดยการเผยแพร่ผ่านทางเว็บไซต์ของมหาวิทยาลัย

๓. กำหนดให้มีผู้รับผิดชอบตามนโยบายและแนวทางปฏิบัติดังกล่าว

๔. มีการกำหนดให้ปรับปรุงนโยบายและแนวทางปฏิบัติ อย่างน้อยปีละ ๑ ครั้ง

/๔.๒ ส่วนที่...

๔.๒ ส่วนที่ว่าด้วยรายละเอียดของนโยบาย

๑. การเข้าถึงหรือควบคุมการใช้งานสารสนเทศ มีนโยบายที่จะให้บริการเทคโนโลยีสารสนเทศแก่ผู้ใช้งานอย่างทั่วถึง โดยให้ผู้ใช้งานสามารถเข้าถึงและใช้งานระบบสารสนเทศได้อย่างสะดวกและรวดเร็ว รวมทั้งการคุ้มครองข้อมูลส่วนบุคคล

๒. มีระบบสารสนเทศและระบบสำรองของสารสนเทศ มีนโยบายในการบริหารจัดการระบบสารสนเทศ โดยมีการแยกประเภทและจัดเก็บเทคโนโลยีสารสนเทศเป็นหมวดหมู่มีระบบสำรองที่พร้อมใช้งาน รวมทั้งมีแผนฉุกเฉินในการใช้งานระบบสารสนเทศได้อย่างต่อเนื่อง

๓. มีการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ มีนโยบายในการตรวจสอบ ประเมินความเสี่ยงและกำหนดมาตรฐานในการควบคุมความเสี่ยงด้านสารสนเทศ อย่างน้อย ปีละ ๑ ครั้ง

๔. การสร้างความรู้ ความเข้าใจในการใช้ระบบสารสนเทศ มีนโยบายในการสร้างความรู้ในการใช้ระบบสารสนเทศ โดยการจัดทำคู่มือการจัดการอบรมเพื่อสร้างความรู้ความเข้าใจในการใช้ระบบสารสนเทศแก่ผู้ใช้งาน

ข้อ ๕ ข้อกำหนดการเข้าถึงและควบคุมการใช้งานสารสนเทศ (access control) ซึ่งมีเนื้อหา ดังนี้

๕.๑ มีการควบคุมการเข้าถึงข้อมูลและอุปกรณ์ในการประมวลผลข้อมูล โดยคำนึงถึงการใช้งานและความมั่นคงปลอดภัย

๕.๒ มีการกำหนดกฎเกณฑ์เกี่ยวกับการอนุญาตให้เข้าถึงโดยการกำหนดตามนโยบายที่เกี่ยวข้องกับการอนุญาต การกำหนดสิทธิ์หรือการมอบอำนาจของหน่วยงาน

๕.๓ มีการกำหนดประเภทของข้อมูล ลำดับความสำคัญหรือลำดับชั้นความลับของข้อมูล รวมทั้งระดับชั้นการเข้าถึง เวลาที่ได้เข้าถึงและช่องทางการเข้าถึง

ข้อ ๖ การบริหารจัดการการเข้าถึงของผู้ใช้งาน (user access management) เพื่อควบคุมการเข้าถึงระบบสารสนเทศเฉพาะผู้ที่ได้รับอนุญาตแล้ว และผ่านการฝึกอบรมหลักสูตรการสร้างความตระหนักเรื่องความมั่นคงปลอดภัยสารสนเทศ (information security awareness training) เพื่อป้องกันการเข้าถึงจากผู้ซึ่งไม่ได้รับอนุญาต ดังนี้

๖.๑ สร้างความรู้ความเข้าใจให้กับผู้ใช้งาน เพื่อให้เกิดความตระหนัก ความเข้าใจถึงภัยและผลกระทบที่เกิดจากการใช้งานระบบสารสนเทศโดยไม่ระมัดระวังหรือรู้เท่าไม่ถึงการณ์ รวมถึงกำหนดให้มีมาตรการเชิงป้องกันตามความเหมาะสม

๖.๒ การลงทะเบียนผู้ใช้งาน (user registration) ต้องกำหนดให้มีขั้นตอนทางปฏิบัติสำหรับการลงทะเบียนผู้ใช้งานเมื่อมีการอนุญาตให้เข้าถึงระบบสารสนเทศ และการตัดออกจากทะเบียนของผู้ใช้งานเมื่อมีการยกเลิกเพิกถอนการอนุญาตดังกล่าว

๖.๓ การบริหารจัดการสิทธิ์ของผู้ใช้งาน (user management) ต้องจัดให้มีการควบคุมและจำกัดสิทธิ์เพื่อเข้าถึงและใช้งานระบบสารสนเทศแต่ละชนิดตามความเหมาะสม

๖.๔ การบริหารจัดการรหัสผ่านสำหรับผู้ใช้งาน (user password management) ต้องจัดให้มีกระบวนการบริหารจัดการรหัสผ่านสำหรับผู้ใช้งานอย่างรัดกุม

๖.๕ การทบทวนสิทธิ์การเข้าถึงของผู้ใช้งาน (review of user access rights) ต้องจัดให้มีกระบวนการทบทวนสิทธิ์การเข้าถึงของผู้ใช้งานระบบสารสนเทศอย่างน้อยปีละ ๑ ครั้ง

/ข้อ ๗...

ข้อ ๗ การกำหนดหน้าที่ความรับผิดชอบของผู้ใช้งาน (user responsibilities) เพื่อป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต การเปิดเผย การล่วงรู้หรือการลักลอบทำสำเนาข้อมูลสารสนเทศ และการลักขโมยอุปกรณ์ประมวลผลสารสนเทศ ดังนี้

๗.๑ การใช้งานรหัสผ่าน (password user) ต้องกำหนดแนวปฏิบัติที่ดีสำหรับผู้ใช้งานในการกำหนดรหัสผ่าน การใช้งานรหัสผ่าน และการเปลี่ยนรหัสผ่านที่มีคุณภาพ

๗.๒ การป้องกันอุปกรณ์ในขณะที่ไม่มีผู้ใช้งาน กำหนดแนวปฏิบัติที่เหมาะสมเพื่อป้องกันไม่ให้ผู้ไม่มีสิทธิ์สามารถเข้าถึงอุปกรณ์ของหน่วยงานในขณะที่ไม่มีผู้ดูแล

๗.๓ การปฏิบัติตามนโยบายควบคุมการไม่ทิ้งสินทรัพย์สารสนเทศและการใช้งานระบบคอมพิวเตอร์ (clear desk and clear screen policy) โดยต้องไม่ให้สินทรัพย์สารสนเทศอยู่ในภาวะซึ่งเสี่ยงต่อการเข้าถึงโดยผู้ซึ่งไม่มีสิทธิ์ และกำหนดให้ผู้ใช้งานออกจากระบบสารสนเทศเมื่อว่างเว้นจากการใช้งาน

๗.๔ การเข้ารหัสของผู้ใช้งานมาใช้กับข้อมูลที่เป็นความลับ โดยให้ปฏิบัติตามระเบียบการรักษาความลับทางราชการ พ.ศ. ๒๕๔๔

ข้อ ๘ การควบคุมการเข้าถึงเครือข่าย (network access control) เพื่อป้องกันการเข้าถึงบริการทางเครือข่ายโดยไม่ได้รับอนุญาต ดังนี้

๘.๑ การใช้งานบริการเครือข่าย ต้องกำหนดให้ผู้ใช้งานสามารถเข้าถึงระบบสารสนเทศได้แต่เพียงบริการที่ได้รับอนุญาตให้เข้าถึงเท่านั้น

๘.๒ การยืนยันตัวบุคคลสำหรับผู้ใช้ที่อยู่ภายนอกหน่วยงาน (user authentication for external connections) ต้องกำหนดให้มีการยืนยันตัวบุคคลก่อนที่จะอนุญาตให้ผู้ใช้ที่อยู่ภายนอกหน่วยงานสามารถเข้าใช้งานเครือข่ายและระบบสารสนเทศได้

๘.๓ การระบุอุปกรณ์บนเครือข่าย (equipment identification in networks) กำหนดวิธีการที่สามารถระบุอุปกรณ์บนเครือข่าย และใช้การระบุอุปกรณ์บนเครือข่ายเป็นการยืนยัน

๘.๔ การป้องกันพอร์ตที่ใช้สำหรับตรวจสอบและปรับแต่งระบบ (remote diagnostic and configuration port protection) ต้องควบคุมการเข้าถึงพอร์ตที่ใช้สำหรับตรวจสอบและปรับแต่งระบบทั้งการเข้าถึงทางกายภาพและทางเครือข่าย

๘.๕ การแบ่งแยกเครือข่าย (segregation in networks) ต้องทำการแบ่งแยกเครือข่ายตามกลุ่มของบริการสารสนเทศ กลุ่มผู้ใช้งาน และกลุ่มของระบบสารสนเทศ

๘.๖ การควบคุมการเชื่อมต่อทางเครือข่าย (network connection control) ต้องควบคุมการเข้าถึงหรือใช้งานเครือข่ายที่มีการใช้ร่วมกัน หรือเชื่อมต่อระหว่างหน่วยงานให้สอดคล้องกับแนวปฏิบัติในการควบคุมการเข้าถึง

๘.๗ การควบคุมการจัดเส้นทางบนเครือข่าย (network routing control) ต้องควบคุมการจัดเส้นทางบนเครือข่ายเพื่อให้การเชื่อมต่อของคอมพิวเตอร์และการส่งผ่าน หรือไหลเวียนของข้อมูล หรือสารสนเทศสอดคล้องกับแนวปฏิบัติในการควบคุมการเข้าถึง หรือการประยุกต์ใช้งานตามภารกิจ

ข้อ ๙ การควบคุมการเข้าถึงระบบปฏิบัติการ (operating system access control) เพื่อป้องกันการเข้าถึงระบบปฏิบัติการโดยไม่ได้รับอนุญาต ดังนี้

๙.๑ การกำหนดขั้นตอนปฏิบัติเพื่อการเข้าใช้งานที่มั่นคงปลอดภัย การเข้าถึงระบบปฏิบัติการจะต้องควบคุมโดยวิธีการยืนยันตัวตนที่มั่นคงปลอดภัย

/๙.๒ การระบุ...

๙.๒ การระบุและยืนยันตัวตนของผู้ใช้งาน (user identification and authentication) ต้องกำหนดให้ผู้ใช้งานมีข้อมูลเฉพาะเจาะจงซึ่งสามารถระบุตัวตนของผู้ใช้งาน และเลือกใช้ขั้นตอนทางเทคนิคในการยืนยันตัวตนที่เหมาะสมเพื่อรองรับการกล่าวอ้างว่าเป็นผู้ใช้งานที่ระบุถึง

๙.๓ การบริหารจัดการรหัสผ่าน (password management system) ต้องมีระบบบริหารจัดการรหัสผ่านที่สามารถทำงานเชิงโต้ตอบ (interactive) หรือมีการทำงานในลักษณะอัตโนมัติ ซึ่งเอื้อต่อการกำหนดรหัสผ่านที่มีคุณภาพ

๙.๔ การใช้งานโปรแกรมอรรถประโยชน์ (user of system utilities) จำกัดและควบคุมการใช้งานโปรแกรมประเภทอรรถประโยชน์ เพื่อป้องกันการละเมิด หรือหลีกเลี่ยงมาตรการความมั่นคงปลอดภัยที่ได้กำหนดไว้

๙.๕ การยุติการใช้งานระบบสารสนเทศ (session time-out) เมื่อว่างเว้นจากการใช้งาน

๙.๖ การจำกัดระยะเวลาการเชื่อมต่อระบบสารสนเทศ (limitation of connection time) จำกัดระยะเวลาในการเชื่อมต่อ เพื่อให้มีความมั่นคงปลอดภัยมากยิ่งขึ้น สำหรับระบบสารสนเทศหรือแอพพลิเคชั่นที่มีความเสี่ยง หรือมีความสำคัญสูง

ข้อ ๑๐ ให้มีการควบคุมการเข้าถึงโปรแกรมประยุกต์ หรือแอพพลิเคชั่นและสารสนเทศ (application and information access control) ดังนี้

๑๐.๑ การจำกัดการเข้าถึงสารสนเทศ (information access restriction) ต้องจำกัดหรือควบคุมการเข้าถึง หรือเข้าใช้งานของผู้ใช้งาน และบุคลากรฝ่ายสนับสนุน การเข้าใช้งานในการเข้าถึงสารสนเทศและฟังก์ชัน (functions) ต่างๆ ของโปรแกรมประยุกต์ หรือแอพพลิเคชั่น โดยต้องสอดคล้องตามนโยบายควบคุมการเข้าถึงสารสนเทศที่ได้กำหนดไว้

๑๐.๒ ระบบซึ่งไวต่อการรบกวน มีผลกระทบและมีความสำคัญสูงต่อองค์กร ต้องได้รับการแยกออกจากระบบอื่น ๆ และมีการควบคุมสภาพแวดล้อมของตนเองโดยเฉพาะ ให้มีการควบคุมอุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่ และการปฏิบัติงานจากภายนอกหน่วยงาน (mobile computing and teleworking)

๑๐.๓ การควบคุมอุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่ ต้องกำหนดข้อปฏิบัติและมาตรการที่เหมาะสมเพื่อปกป้องสารสนเทศจากความเสี่ยงของการใช้อุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่

๑๐.๔ การปฏิบัติงานจากภายนอกสำนักงาน (teleworking) ต้องกำหนดข้อปฏิบัติ แผนงาน และขั้นตอนปฏิบัติเพื่อปรับใช้สำหรับการปฏิบัติงานขององค์กรจากภายนอกหน่วยงาน

ข้อ ๑๑ การจัดทำระบบสำรองของระบบสารสนเทศ ตามแนวทางต่อไปนี้

๑๑.๑ ต้องพิจารณาคัดเลือก และจัดทำระบบสำรองที่เหมาะสมให้อยู่ในสภาพพร้อมใช้งาน

๑๑.๒ ต้องจัดทำแผนเตรียมความพร้อมกรณีฉุกเฉิน ในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์ เพื่อให้สามารถใช้งานสารสนเทศได้ตามปกติอย่างต่อเนื่อง และปรับปรุงแผนเตรียมความพร้อมกรณีฉุกเฉินดังกล่าว ให้สามารถใช้ได้อย่างเหมาะสมและสอดคล้องกับการใช้งานตามภารกิจ

๑๑.๓ ต้องมีการกำหนดหน้าที่และความรับผิดชอบของบุคลากร ซึ่งดูแลรับผิดชอบระบบสารสนเทศ ระบบสำรอง และการจัดทำแผนเตรียมพร้อมกรณีฉุกเฉินในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์

๑๑.๔ ต้องมีการทดสอบสภาพพร้อมใช้งานของระบบสารสนเทศ ระบบสำรอง และระบบแผนเตรียมพร้อมกรณีฉุกเฉิน อย่างน้อยปีละ ๑ ครั้ง

๑๑.๕ ต้องมีการปฏิบัติและทบทวนแนวทางจัดทำระบบสำรอง อย่างน้อยปีละ ๑ ครั้ง

/ข้อ ๑๒...

ข้อ ๑๒ มีการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ ดังนี้

๑๒.๑ ต้องจัดให้มีการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศที่อาจเกิดขึ้นกับระบบสารสนเทศ (information security audit and assessment) อย่างน้อยปีละ ๑ ครั้ง

๑๒.๒ การตรวจสอบและประเมินความเสี่ยงจะต้องดำเนินการโดยหน่วยตรวจสอบภายใน (internal auditor) เพื่อให้มหาวิทยาลัยได้ทราบถึงระดับความเสี่ยง และระดับความมั่นคงปลอดภัยของสารสนเทศ

ข้อ ๑๓ การกำหนดความรับผิดชอบ กรณีระบบคอมพิวเตอร์หรือข้อมูลสารสนเทศเกิดความเสียหาย หรืออันตรายแก่มหาวิทยาลัย หรือผู้หนึ่งผู้ใด อันเนื่องมาจากความบกพร่อง ละเลย หรือฝ่าฝืนการปฏิบัติตามนโยบายและข้อปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ โดยกำหนดให้ผู้บริหารระดับสูง ซึ่งมีหน้าที่ดูแลรับผิดชอบด้านสารสนเทศของมหาวิทยาลัยเป็นผู้รับผิดชอบต่อความเสี่ยง ความเสียหายหรืออันตรายที่เกิดขึ้น

ข้อ ๑๔ ให้อธิการบดีรักษาการตามประกาศนี้ กรณีเกิดปัญหาในการใช้ประกาศนี้ ให้อธิการบดีมีอำนาจวินิจฉัยสั่งการ

ประกาศนี้ ให้มีผลใช้บังคับตั้งแต่วันประกาศ เป็นต้นไป

ประกาศ ณ วันที่ ๓๑ มกราคม พ.ศ. ๒๕๖๑

(รองศาสตราจารย์จิระพันธ์ ห้วยแสน)
อธิการบดีมหาวิทยาลัยกาฬสินธุ์