

(สำเนา)  
ประกาศมหาวิทยาลัยสงขลานครินทร์  
เรื่อง นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ  
มหาวิทยาลัยสงขลานครินทร์ พ.ศ.๒๕๕๘

.....

เพื่อให้การบริหารจัดการและการพัฒนาระบบเทคโนโลยีสารสนเทศของมหาวิทยาลัยสงขลานครินทร์ เป็นไปอย่างเหมาะสม มีประสิทธิภาพ มีความมั่นคงปลอดภัย มีความเชื่อถือได้ และสามารถให้บริการได้อย่างต่อเนื่อง รวมทั้งสามารถป้องกันปัญหาที่อาจเกิดขึ้นจากการใช้งานระบบเทคโนโลยีสารสนเทศในลักษณะที่ไม่ถูกต้องและการถูกคุกคามจากภัยต่าง ๆ ซึ่งอาจก่อให้เกิดความเสียหายแก่มหาวิทยาลัยและหน่วยงานในสังกัด อีกทั้งเป็นการดำเนินการให้สอดคล้องตามมาตรา ๕ และมาตรา ๗ แห่งพระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ. ๒๕๔๙ ซึ่งกำหนดให้หน่วยงานของรัฐจัดทำประกาศนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ จึงอาศัยอำนาจตามความในมาตรา ๒๑(๑) แห่งพระราชบัญญัติมหาวิทยาลัยสงขลานครินทร์ พ.ศ. ๒๕๒๒ ออกประกาศไว้ ดังนี้

ข้อ ๑ ประกาศนี้เรียกว่า “ประกาศมหาวิทยาลัยสงขลานครินทร์ เรื่อง นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศมหาวิทยาลัยสงขลานครินทร์ พ.ศ. ๒๕๕๘

ข้อ ๒ ในประกาศนี้

- ๒.๑. “มหาวิทยาลัย” หมายถึง มหาวิทยาลัยสงขลานครินทร์
- ๒.๒. “ผู้บริหาร” หมายถึง อธิการบดี รองอธิการบดี ผู้ช่วยอธิการบดี หรือผู้ที่อธิการบดีมอบหมายให้ดูแลรับผิดชอบงานด้านเทคโนโลยีสารสนเทศของมหาวิทยาลัย
- ๒.๓. “ผู้บริหารระดับสูงสุดของหน่วยงาน” (Chief Executive Officer:CEO) หมายถึง อธิการบดี
- ๒.๔. “นโยบาย” หมายถึง นโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ
- ๒.๕. “ผู้ใช้งาน” หมายถึง บุคลากรและนักศึกษาของมหาวิทยาลัย รวมถึงบุคคล และ/หรือ บุคคลหรือหน่วยงานภายนอกที่ได้รับอนุญาตให้ใช้เครื่องคอมพิวเตอร์ ระบบเครือข่าย และโปรแกรมประยุกต์หรือแอปพลิเคชันของมหาวิทยาลัย
- ๒.๖. “สิทธิ์ของผู้ใช้งาน” หมายถึง สิทธิ์ทั่วไป สิทธิ์จำเพาะ สิทธิ์พิเศษ และสิทธิ์อื่นใดที่เกี่ยวข้องกับระบบสารสนเทศของมหาวิทยาลัย
- ๒.๗. “สินทรัพย์” (asset) หมายถึง ข้อมูล ระบบข้อมูล และอุปกรณ์ด้านเทคโนโลยีสารสนเทศและการสื่อสารของมหาวิทยาลัย เช่น อุปกรณ์ระบบเครือข่าย ซอฟต์แวร์ที่มีลิขสิทธิ์ เป็นต้น
- ๒.๘. “การเข้าถึงหรือควบคุมการใช้งานสารสนเทศ” หมายถึง การอนุญาต การกำหนดสิทธิ์ หรือการมอบอำนาจให้ผู้ใช้งาน เข้าถึงหรือใช้งานเครือข่ายหรือระบบสารสนเทศ ทั้งทางอิเล็กทรอนิกส์และทางกายภาพ
- ๒.๙. “ความมั่นคงปลอดภัยด้านสารสนเทศ” (information security) หมายถึง การดำรงไว้ซึ่งความลับ (confidentiality) ความถูกต้องครบถ้วน (integrity) และสภาพพร้อมใช้งาน (availability) ของสารสนเทศรวมทั้งคุณสมบัติอื่น ได้แก่ ความถูกต้องแท้จริง

(authenticity) ความรับผิดชอบ (accountability) การห้ามปฏิเสธความรับผิดชอบ (non-repudiation) และความน่าเชื่อถือ (reliability)

๒.๑๐. “เหตุการณ์ด้านความมั่นคงปลอดภัย” (information security event) หมายถึง กรณีที่ระบุการเกิดเหตุการณ์ สภาพของบริการหรือเครือข่าย ที่แสดงให้เห็นความเป็นไปได้ที่จะเกิดการฝ่าฝืนนโยบายด้านความมั่นคงปลอดภัยหรือมาตรการป้องกันที่ล้มเหลว หรือเหตุการณ์อื่นไม่อาจรู้ได้ว่าอาจเกี่ยวข้องกับความปลอดภัย

๒.๑๑. “สถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด”

(information security incident) หมายถึง สถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด (unwanted or unexpected) ซึ่งอาจทำให้ระบบขององค์กรถูกรบกวนหรือโจมตี และความปลอดภัยถูกคุกคาม

ข้อ ๓ การรักษาความมั่นคงปลอดภัยด้านสารสนเทศตามประกาศฉบับนี้ มีเนื้อหาประกอบด้วย

๓.๑. นโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ มีเนื้อหาครอบคลุมตามข้อ ๔

๓.๒. แนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ มีเนื้อหาครอบคลุมตามข้อ ๕ ถึงข้อ ๑๑

ข้อ ๔ นโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ตามประกาศนี้มี ๒ ส่วน ดังนี้

๔.๑. ส่วนที่ว่าด้วยการจัดทำนโยบาย

๔.๑.๑. ผู้บริหาร เจ้าหน้าที่ปฏิบัติการด้านคอมพิวเตอร์และผู้ใช้งานมีส่วนร่วมในการทำนโยบาย

๔.๑.๒. นโยบายได้ทำเป็นลายลักษณ์อักษร โดยประกาศให้ผู้ใช้งานทราบและสามารถเข้าถึงได้อย่างสะดวกผ่านทางเว็บไซต์ของมหาวิทยาลัย

๔.๑.๓. กำหนดผู้รับผิดชอบตามนโยบายและแนวปฏิบัติดังกล่าวให้ชัดเจน

๔.๑.๔. ต้องทบทวนและปรับปรุงนโยบายอย่างน้อยปีละ ๑ ครั้ง

๔.๒. ส่วนที่ว่าด้วยรายละเอียดของนโยบาย

๔.๒.๑. การเข้าถึงและการควบคุมการใช้งานสารสนเทศ มีนโยบายที่จะให้บริการเทคโนโลยีสารสนเทศแก่ผู้ใช้งานและประชาชนอย่างทั่วถึง เพื่อให้ผู้ใช้งานสามารถเข้าถึงและใช้งานระบบสารสนเทศได้อย่างสะดวก รวดเร็ว และให้ความคุ้มครองข้อมูลที่ไม่พึงเปิดเผย

๔.๒.๒. มีระบบสารสนเทศและระบบสำรองของสารสนเทศ มีนโยบายในการบริหารจัดการระบบสารสนเทศที่ได้มาตรฐาน โดยแยกประเภทและจัดเก็บเป็นหมวดหมู่มีระบบสำรองระบบสารสนเทศและระบบคอมพิวเตอร์ที่สมบูรณ์และสภาพพร้อมใช้งาน และมีแผนฉุกเฉินเพื่อให้ระบบสามารถทำงานได้อย่างต่อเนื่อง

๔.๒.๓. การตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ ต้องดำเนินการอย่างสม่ำเสมอ โดยกำหนดให้ต้องตรวจสอบ ควบคุมคุณภาพ และดำเนินการตรวจประเมินระบบรักษาความมั่นคงปลอดภัยของระบบสารสนเทศอย่างน้อยปีละ ๑ ครั้ง

- ๔.๒.๔. กำหนดหน้าที่และความรับผิดชอบเกี่ยวกับการรายงานเหตุการณ์ที่เสี่ยงต่อความมั่นคงปลอดภัยที่เกิดขึ้น
- ๔.๒.๕. การสร้างความรู้ความเข้าใจการใช้งานระบบสารสนเทศหรือระบบคอมพิวเตอร์ มีนโยบายในการสร้างความรู้ความเข้าใจ โดยการจัดทำคู่มือ การฝึกอบรมและเผยแพร่การใช้งานระบบสารสนเทศและระบบคอมพิวเตอร์แก่ผู้ใช้งาน

**ข้อ ๕** ข้อกำหนดการเข้าถึงหรือควบคุมการใช้งานระบบสารสนเทศ

- ๕.๑. ต้องควบคุมการเข้าถึงข้อมูลและอุปกรณ์ในการประมวลผลข้อมูลโดยคำนึงถึงการใช้งานและความมั่นคงปลอดภัย
- ๕.๒. กำหนดหลักเกณฑ์เกี่ยวกับการอนุญาตให้เข้าถึงตามนโยบายที่เกี่ยวข้องกับการอนุญาต การกำหนดสิทธิ์ หรือการมอบอำนาจของหน่วยงาน
- ๕.๓. กำหนดประเภทของข้อมูล ลำดับความสำคัญ หรือลำดับชั้นความลับของข้อมูล รวมทั้งระดับชั้นการเข้าถึง เวลาที่เข้าถึงได้ และช่องทางการเข้าถึง
- ๕.๔. มีวิธีการบริหารจัดการการเข้าถึงข้อมูลสารสนเทศและระบบสารสนเทศของผู้ใช้งานแต่ละประเภทที่เหมาะสมและตรวจสอบได้ เพื่อป้องกันการเข้าถึงผู้ไม่ได้รับอนุญาต โดยครอบคลุมการลงทะเบียน การจัดการสิทธิผู้ใช้งาน รหัสผ่าน การทบทวนสิทธิการใช้งาน เพื่อให้มั่นใจว่าสอดคล้องกับภาระหน้าที่และความจำเป็นในการใช้งาน
- ๕.๕. ต้องควบคุมการเข้าถึงเครือข่ายและการใช้บริการผ่านเครือข่าย รวมทั้งการเชื่อมต่อเครือข่ายทั้งจากภายในสำนักงานและจากภายนอกสำนักงาน เพื่อป้องกันการเข้าถึงข้อมูลสารสนเทศหรือระบบสารสนเทศโดยไม่ได้รับอนุญาต
- ๕.๖. ต้องควบคุมการเข้าถึงระบบปฏิบัติการ เพื่อป้องกันการใช้งานอุปกรณ์เพื่อการเข้าถึงข้อมูลสารสนเทศโดยไม่ได้รับอนุญาต
- ๕.๗. ต้องควบคุมการเข้าถึงโปรแกรมและระบบสารสนเทศ เพื่อป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต

**ข้อ ๖** ต้องบริหารจัดการการเข้าถึงของผู้ใช้งาน เพื่อควบคุมการเข้าถึงระบบสารสนเทศเฉพาะผู้ที่ได้รับอนุญาตแล้ว และผ่านการฝึกอบรมหลักสูตรการสร้างความรู้ความตระหนักเรื่องความมั่นคงปลอดภัยสารสนเทศ เพื่อป้องกันการเข้าถึงจากผู้ซึ่งไม่ได้รับอนุญาต ดังนี้

- ๖.๑. สร้างความรู้ความเข้าใจให้กับผู้ใช้งาน เพื่อให้เกิดความตระหนัก ความเข้าใจถึงภัยและผลกระทบที่เกิดจากการใช้งานระบบสารสนเทศโดยไม่ระมัดระวังหรือรู้เท่าไม่ถึงการณ์ รวมถึงกำหนดให้มีมาตรการเชิงป้องกันตามความเหมาะสม
- ๖.๒. การลงทะเบียนผู้ใช้งาน ต้องกำหนดให้มีขั้นตอนปฏิบัติสำหรับการลงทะเบียนผู้ใช้งานเมื่อต้องอนุญาตให้เข้าถึงระบบสารสนเทศ และการตัดออกจากทะเบียนของผู้ใช้งานเมื่อยกเลิกการอนุญาตดังกล่าว
- ๖.๓. การปฏิบัติตามนโยบายควบคุมการไม่ทิ้งสินทรัพย์สารสนเทศสำคัญไว้ในที่ที่ไม่ปลอดภัย โดยต้องควบคุมไม่ให้สินทรัพย์สารสนเทศ เช่น เอกสาร สื่อบันทึกข้อมูล คอมพิวเตอร์ สารสนเทศ ฯลฯ อยู่ในภาวะเสี่ยงต่อการเข้าถึงโดยผู้ซึ่งไม่มีสิทธิ์และต้องกำหนดให้ผู้ใช้งานออกจากระบบสารสนเทศเมื่อว่างเว้นจากการใช้งาน

๖.๔. ผู้ใช้งานอาจนำการเข้ารหัสมาใช้กับข้อมูลที่เป็นความลับ โดยให้ปฏิบัติตามระเบียบว่าด้วยการรักษาความลับของทางราชการ พ.ศ. ๒๕๔๔

**ข้อ ๗** ต้องกำหนดหน้าที่ความรับผิดชอบของผู้ใช้งาน เพื่อป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต การเปิดเผย การลวงรู้ หรือการลักลอบทำสำเนาข้อมูลสารสนเทศและการลักขโมยอุปกรณ์ประมวลผลสารสนเทศมีเนื้อหา ดังนี้

- ๗.๑. การใช้งานรหัสผ่าน กำหนดแนวปฏิบัติที่ดีสำหรับผู้ใช้งานในการกำหนดรหัสผ่าน การใช้งานรหัสผ่าน และการเปลี่ยนรหัสผ่านที่มีคุณภาพ
- ๗.๒. การป้องกันอุปกรณ์ในขณะที่ไม่มีผู้ใช้งาน ต้องกำหนดแนวปฏิบัติที่เหมาะสมเพื่อป้องกันไม่ให้ผู้ไม่มีสิทธิ์สามารถเข้าถึงอุปกรณ์ของหน่วยงานในขณะที่ไม่มีผู้ดูแล
- ๗.๓. การปฏิบัติตามนโยบายควบคุมการไม่ทิ้งสินทรัพย์สารสนเทศสำคัญไว้ในที่ที่ไม่ปลอดภัย โดยต้องควบคุมไม่ให้สินทรัพย์สารสนเทศ เช่น เอกสาร สื่อบันทึกข้อมูล คอมพิวเตอร์ สารสนเทศ ฯลฯ อยู่ในภาวะเสี่ยงต่อการเข้าถึงโดยผู้ซึ่งไม่มีสิทธิ์และต้องกำหนดให้ผู้ใช้งานออกจากระบบสารสนเทศเมื่อไม่ใช้งาน

**ข้อ ๘** การจัดทำระบบสำรองสำหรับระบบสารสนเทศ ตามแนวทางต่อไปนี้

- ๘.๑. ต้องพิจารณาคัดเลือกและจัดทำระบบสำรองให้อยู่ในสภาพพร้อมใช้งาน
- ๘.๒. ต้องจัดทำแผนเตรียมความพร้อมกรณีฉุกเฉินในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์ เพื่อให้สามารถใช้งานได้ตามปกติอย่างต่อเนื่อง โดยต้องปรับปรุงแผนเตรียมความพร้อมกรณีฉุกเฉินดังกล่าวให้สามารถปรับใช้ได้อย่างเหมาะสมและสอดคล้องกับการทำงานตามภารกิจ
- ๘.๓. ต้องกำหนดหน้าที่และความรับผิดชอบของบุคลากรซึ่งดูแลรับผิดชอบระบบสารสนเทศ ระบบสำรอง และจัดทำแผนเตรียมความพร้อมกรณีฉุกเฉินในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการอิเล็กทรอนิกส์
- ๘.๔. ต้องทดสอบสภาพพร้อมใช้งานของระบบสารสนเทศ ระบบสำรองและแผนเตรียมความพร้อมกรณีฉุกเฉินอย่างสม่ำเสมอ ปีละ 1 ครั้ง
- ๘.๕. ต้องปฏิบัติและทบทวนแนวทางการจัดทำระบบสำรอง ปีละ 1 ครั้ง

**ข้อ ๙** การตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ โดยมีเนื้อหา ดังนี้

- ๙.๑. กำหนดให้ตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศที่อาจเกิดขึ้นกับระบบสารสนเทศปีละ 1 ครั้ง
- ๙.๒. ในการตรวจสอบและประเมินความเสี่ยงจะต้องดำเนินการโดยหน่วยตรวจสอบภายในมหาวิทยาลัยสงขลานครินทร์ เพื่อให้หน่วยงานได้ทราบถึงระดับความเสี่ยงและระดับความมั่นคงปลอดภัยสารสนเทศ

**ข้อ ๑๐** ต้องประกาศนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศให้ผู้เกี่ยวข้องทราบ เพื่อให้สามารถเข้าถึง เข้าใจ และปฏิบัติตามนโยบายและแนวปฏิบัติ ด้วยวิธีการใดวิธีการหนึ่ง ดังนี้

- ๑๐.๑. หนังสือเวียนภายในองค์กร
- ๑๐.๒. เว็บไซต์ภายในมหาวิทยาลัยสงขลานครินทร์

ข้อ ๑๑ หน่วยงานภายในมหาวิทยาลัยที่ต้องบริหารจัดการระบบเทคโนโลยีสารสนเทศสามารถกำหนดแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานได้เอง ทั้งนี้ ต้องให้สอดคล้องกับนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ มหาวิทยาลัยสงขลานครินทร์ พ.ศ.๒๕๕๘

ข้อ ๑๒ หากระบบคอมพิวเตอร์หรือข้อมูลสารสนเทศเกิดความเสียหายหรืออันตรายใด ๆ แก่องค์กรหรือผู้หนึ่งผู้ใด อันเนื่องมาจากความบกพร่อง ละเลย หรือฝ่าฝืนการปฏิบัติตามนโยบาย และแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศให้ผู้บริหารระดับสูงสุดของหน่วยงาน (Chief Executive Officer: CEO) เป็นผู้รับผิดชอบต่อความเสี่ยง ความเสียหาย หรืออันตรายที่เกิดขึ้น

ข้อ ๑๓ ให้ศูนย์คอมพิวเตอร์ เป็นผู้รับผิดชอบดำเนินการให้เป็นไปตามประกาศนี้ และกำหนดให้ทบทวนนโยบายและแนวปฏิบัติให้เป็นปัจจุบันอย่างน้อยปีละ ๑ ครั้ง

ข้อ ๑๔ ประกาศนี้ให้ใช้บังคับตั้งแต่วันที่ประกาศเป็นต้นไป

ประกาศ ณ วันที่ ๒๔ มิถุนายน ๒๕๕๘

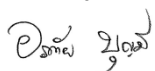
(ลงชื่อ)

ชูศักดิ์ ลิ้มสกุล

(รองศาสตราจารย์ ดร.ชูศักดิ์ ลิ้มสกุล)

อธิการบดี

สำเนาถูกต้อง



(นางอรัทัย บุญมี)

นักวิเคราะห์นโยบายและแผนชำนาญการพิเศษ