ประกาศมหาวิทยาลัยสงขลานครินทร์

เรื่อง นโยบายธรรมาภิบาลข้อมูล (Data Governance Policy) มหาวิทยาลัยสงขลานครินทร์

เพื่อให้มหาวิทยาลัยสงขลานครินทร์ มีนโยบายธรรมาภิบาลข้อมูล และการบริหารจัดการข้อมูลเป็นไปอย่างเหมาะสม ข้อมูลมีคุณภาพ มีความมั่นคงปลอดภัย และสามารถดำเนินการได้อย่างต่อเนื่องด้วยความเรียบร้อย ป้องกันปัญหาที่อาจเกิดขึ้นจากภัยคุกคามของการบริหารจัดการข้อมูล รวมทั้งเพื่อให้ผู้บริหาร เจ้าหน้าที่ ผู้รับบริการและผู้ที่เกี่ยวข้องกับมหาวิทยาลัยสงขลานครินทร์ ได้รับทราบ เข้าใจ และถือปฏิบัติเกี่ยวกับธรรมาภิบาลข้อมูลให้เป็นในทิศทางเดียวกัน ตลอดจนให้เกิดความสอดคล้องกับภารกิจของมหาวิทยาลัยสงขลานครินทร์ พระราชบัญญัติการบริหารงานและการให้บริการของภาครัฐผ่านระบบดิจิทัล พ.ศ. ๒๕๖๒ และประกาศคณะกรรมการพัฒนารัฐบาลดิจิทัล เรื่อง ธรรมาภิบาลข้อมูลภาครัฐ

อาศัยอำนาจตามความในมาตรา ๓๔ และมาตรา ๓๙ แห่งพระราชบัญญัติมหาวิทยาลัยสงขลานครินทร์ พ.ศ. ๒๕๕๙ ประกอบกับมาตรา ๖ และมาตรา ๗ แห่งพระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ. ๒๕๔๙ ประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง แนวนโยบายและแนวปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคลของหน่วยงานของรัฐ พ.ศ. ๒๕๕๓ มหาวิทยาลัยสงขลานครินทร์จึงออกประกาศไว้ ดังต่อไปนี้

ข้อ ๑ ประกาศนี้เรียกว่า “ประกาศมหาวิทยาลัยสงขลานครินทร์ เรื่อง นโยบายธรรมาภิบาลข้อมูล (Data Governance Policy) มหาวิทยาลัยสงขลานครินทร์”

ข้อ ๒ ในประกาศนี้

“มหาวิทยาลัย” หมายถึง มหาวิทยาลัยสงขลานครินทร์

“นโยบาย” หมายถึง หลักการเกี่ยวกับธรรมาภิบาลข้อมูลที่มหาวิทยาลัยสงขลานครินทร์กำหนดขึ้น

“แนวปฏิบัติ” หมายถึง ข้อปฏิบัติที่มหาวิทยาลัยสงขลานครินทร์กำหนดให้ผู้เกี่ยวข้องถือปฏิบัติ เพื่อให้สามารถบรรลุวัตถุประสงค์และเป้าหมายด้านธรรมาภิบาลข้อมูลตามที่กำหนดไว้

“ธรรมาภิบาลข้อมูลภาครัฐ (Data Governance)” หมายถึง การกำหนดสิทธิ หน้าที่ และความรับผิดชอบของผู้มีส่วนได้ เสียในการบริหารจัดการข้อมูลภาครัฐทุกขั้นตอน เพื่อให้การได้มาและการนำข้อมูลของหน่วยงานของรัฐไปใช้ อย่างถูกต้อง ครบถ้วน เป็นปัจจุบัน รักษาความเป็นส่วนบุคคล และสามารถเชื่อมโยงแลกเปลี่ยน และบูรณาการระหว่างกันได้อย่างมีประสิทธิภาพและมั่นคงปลอดภัย โดยใช้ข้อมูลเป็นหลักในการบริหารงานภาครัฐและการบริการสาธารณะ

“คณะกรรมการธรรมาภิบาลข้อมูล (Data Governance Committee)” หมายถึง กลุ่มบุคคลที่ได้รับมอบหมายในการผลักดัน ส่งเสริมให้เกิดธรรมาภิบาลข้อมูล โดยมีหน้าที่รับผิดชอบในการกำหนดเป้าหมาย กำกับดูแลและติดตามการดำเนินงาน รวมถึงให้คำปรึกษาและตัดสินประเด็นสำคัญที่เกี่ยวข้องกับข้อมูล สนับสนุนส่งเสริม ผลักดันธรรมาภิบาลข้อมูล สื่อสารให้บุคลากรในมหาวิทยาลัยตระหนักถึงความสำคัญของข้อมูลและการใช้ข้อมูลอย่างปลอดภัย

“คณะบริกรข้อมูล (Data Steward Team)” หมายถึง กลุ่มบุคคลที่ได้รับมอบหมายให้ดำเนินงานด้านการกำหนด ทบทวนในเรื่องนโยบาย ทิศทาง หรือมาตรฐานของแนวทางปฏิบัติที่เกี่ยวกับข้อมูลภายในมหาวิทยาลัย ประเมินความเสี่ยงด้านข้อมูล สื่อสารผลักดันการใช้แนวปฏิบัติทางด้านข้อมูลภายในองค์กร ติดตามธรรมาภิบาลข้อมูลขององค์กร และรายงานผลต่อคณะกรรมการธรรมาภิบาลข้อมูล

“ข้อมูล (Data)” หมายถึง สิ่งที่สื่อความหมายให้รู้เรื่องราวข้อเท็จจริงหรือเรื่องอื่นใด ไม่ว่าการสื่อความหมายนั้นจะทำได้โดยสภาพของสิ่งนั้นเองหรือโดยผ่านวิธีการใด ๆ และไม่ว่าจะได้จัดทำไว้ในรูปของเอกสาร แฟ้ม รายงาน หนังสือ แผนผัง แผนที่ ภาพวาด ภาพถ่าย ภาพถ่ายดาวเทียม ฟิล์ม การบันทึกภาพหรือเสียง การบันทึกโดยเครื่องคอมพิวเตอร์ เครื่องมือตรวจวัด การสำรวจระยะไกล หรือวิธีอื่นใดที่ทำให้สิ่งที่บันทึกไว้ปรากฏได้ และให้หมายความรวมถึงข้อมูลอิเล็กทรอนิกส์ตามกฎหมายว่าด้วยธุรกรรมอิเล็กทรอนิกส์

“ข้อมูลหลัก (Master Data)” หมายถึง ข้อมูลที่สร้างและใช้งานร่วมกันภายในขอบเขตการดำเนินงานตามภารกิจของหน่วยงาน เช่น ข้อมูลบุคลากร ข้อมูลการลา ข้อมูลนักศึกษา ข้อมูลการลงทะเบียน

“ชุดข้อมูล (Datasets)” หมายถึง การนำข้อมูลจากหลายแหล่งมารวบรวมเพื่อจัดเป็นชุดให้ตรงตามลักษณะโครงสร้างของข้อมูล

“คำอธิบายชุดข้อมูล/เมทาดาตา (Metadata)” หมายถึง ข้อมูลที่ใช้กำกับและอธิบายข้อมูลหลักหรือกลุ่มของข้อมูลอื่น เป็นคำอธิบายชุดข้อมูลดิจิทัล เพื่อให้ทราบรายละเอียดเกี่ยวกับโครงสร้างของข้อมูล เนื้อหาสาระ รูปแบบการจัดเก็บ แหล่งข้อมูล และสิทธิในการเข้าถึงข้อมูล

“การบริหารจัดการข้อมูล (Data Management)” หมายถึง คำจำกัดความที่อธิบายถึงกระบวนการที่ใช้ในการวางแผน (Plan) การระบุชี้ชัด (Specify) การเปิดใช้งาน (Enable) การสร้าง (Create) การรับ (Acquire) การดูแลรักษา (Maintain) การใช้งาน (Use) การจัดเก็บถาวร (Archive) การเรียกใช้ดึงข้อมูล (Retrieve) การควบคุม (Control) และการทำลายข้อมูล (Purge)

“การบริหารจัดการคุณภาพของข้อมูล (Data Quality Management)” หมายถึง การกำหนดมาตรฐานและระเบียบแนวปฏิบัติการบริหารจัดการคุณภาพข้อมูล ครอบคลุมบทบาทหน้าที่ ผู้รับผิดชอบการบริหารจัดการ คุณลักษณะข้อมูลที่มีคุณภาพ และกระบวนการบริหารจัดการคุณภาพข้อมูล

“การจัดการวงจรชีวิตข้อมูล (Data Lifecycle Management)” หมายถึง ลำดับขั้นตอนของข้อมูล ตั้งแต่เริ่มสร้างข้อมูลไปจนถึงการทำลายข้อมูล ประกอบด้วย ๖ ขั้นตอน ดังนี้ การสร้างข้อมูล (Data Creation) การจัดเก็บข้อมูล (Data Storage) การใช้ข้อมูล (Data Usage) การเผยแพร่ข้อมูล (Data Dissemination) การจัดเก็บข้อมูลถาวร (Data Archival) และการทำลายข้อมูล (Data Destruction)

“ความมั่นคงปลอดภัยของข้อมูล (Data Security)” หมายถึง การป้องกันข้อมูลในบริบทของการรักษาความลับ ความถูกต้องของข้อมูล ความพร้อมใช้งานของข้อมูลเป็นการธำรงไว้ซึ่งความลับ ความถูกต้องครบถ้วน และการรักษาสภาพพร้อมใช้ของข้อมูล รวมทั้งคุณสมบัติอื่น ได้แก่ ความถูกต้องแท้จริง ความรับผิด การห้ามปฏิเสธความรับผิด และความน่าเชื่อถือ

“ระดับชั้นความลับ” หมายถึง การกำหนดการเปิดเผยข้อมูลต่อผู้อื่นให้เหมาะสมกับสถานะการใช้งาน ได้แก่ ลับที่สุด (TOP SECRET) ลับมาก (SECRET) ลับ (CONFIDENTIAL) และเปิดเผยได้

“ผู้ถือข้อมูล (Data Owner)” หมายถึง บุคคลหรือหน่วยงานซึ่งรวมถึงผู้บังคับบัญชาของผู้ถือข้อมูลนั้นด้วยซึ่งมีหน้าที่รับผิดชอบเกี่ยวกับข้อมูลของมหาวิทยาลัยสงขลานครินทร์ที่สามารถบริหารจัดการและควบคุมชุดข้อมูล สร้าง แก้ไข ลบ กำหนดสิทธิ์การเข้าถึง อนุญาต หรือปฏิเสธการเข้าถึงข้อมูล และเป็นผู้รับผิดชอบต่อความถูกต้อง ทันสมัย ความสมบูรณ์ และการทำลาย รวมถึงกำหนดระดับชั้นความลับ สิทธิ์การใช้งาน และความปลอดภัยของข้อมูล

“ผู้ใช้ข้อมูล (Data User)” หมายถึง ผู้ที่ได้รับสิทธิ์การเข้าถึงข้อมูล หรือได้รับมอบหมายสิทธิ์ให้ใช้ข้อมูลของมหาวิทยาลัยสงขลานครินทร์ และสิทธิ์อื่นใดที่เกี่ยวข้องกับระบบสารสนเทศของมหาวิทยาลัยสงขลานครินทร์ รวมถึงผู้ซึ่งได้รับความยินยอมให้ทำงานหรือทำผลประโยชน์ให้แก่มหาวิทยาลัยสงขลานครินทร์

“เจ้าของระบบสารสนเทศ (System Owner)” หมายถึง ผู้ที่มีหน้าที่รับผิดชอบในการใช้งาน ดูแลและบำรุงรักษา หรือปรับปรุงระบบงานที่ใช้ในหน่วยงาน ตามที่มหาวิทยาลัยสงขลานครินทร์กำหนด

“ข้อมูลส่วนบุคคล (Personal Data)” หมายถึง ข้อมูลเกี่ยวกับบุคคลซึ่งทำให้สามารถระบุตัวบุคคลนั้นได้ไม่ว่าทางตรงหรือทางอ้อม แต่ไม่รวมถึงข้อมูลของผู้ถึงแก่กรรมโดยเฉพาะ

“การรักษาความเป็นส่วนบุคคลของข้อมูล (Data Privacy)” หมายถึง การรักษาความเป็นส่วนบุคคลของข้อมูลตามที่กำหนดไว้ในกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล

“การประมวลผลข้อมูลส่วนบุคคล (Personal Data Processing)” หมายถึง การดำเนินการใด ๆ ซึ่งกระทำต่อข้อมูลส่วนบุคคลหรือชุดข้อมูลส่วนบุคคล ไม่ว่าโดยวิธีการอัตโนมัติหรือไม่ เช่น การรวบรวม การบันทึก การถือครองการใช้งานการจัดการ การเก็บ การปรับเปลี่ยน การเผยแพร่ การลบหรือทำลาย

“การจัดจำแนกข้อมูล (Data Classification)” หมายถึง กระบวนการที่ใช้แบ่งข้อมูลออกเป็นระดับต่าง ๆ เพื่อบรรลุวัตถุประสงค์ด้านความปลอดภัยและการเข้าถึงข้อมูลอย่างถูกต้องเหมาะสม

“การถ่ายโอนข้อมูล (Data Transfer)” หมายถึง กระบวนการย้ายข้อมูลจากแหล่งหนึ่งไปยังอีกแหล่งหนึ่งภายใต้การควบคุมของ Data Governance เพื่อให้ข้อมูลยังคงมีคุณภาพและรักษาความปลอดภัยได้

“การแบ่งปันข้อมูล (Data Sharing)” หมายถึง การเปิดเผยข้อมูลระหว่างส่วนต่าง ๆ ภายในองค์กร และรวมถึงการเปิดเผยแก่บุคคลที่สามภายนอกองค์กรภายใต้การควบคุมของ Data Governance เพื่อให้ข้อมูลยังคงมีคุณภาพและรักษาความปลอดภัยได้

ข้อ ๓ นโยบายธรรมาภิบาลข้อมูล (Data Governance Policy) มหาวิทยาลัยสงขลานครินทร์ ประกอบด้วย ๖ นโยบาย ได้แก่ นโยบายธรรมาภิบาลข้อมูล (Data Governance Policy) นโยบายคุณภาพข้อมูล (Data Quality Policy) นโยบายการเชื่อมโยงและการแบ่งปันข้อมูล (Data Transfer and Sharing Policy) นโยบายการจัดชั้นความลับข้อมูล (Data Classification Policy) นโยบายความเป็นส่วนบุคคลและความปลอดภัยของข้อมูล (Data Privacy and Security Policy) และนโยบายการเปิดเผยข้อมูล (Data Disclosure Policy) มีรายละเอียด ดังนี้

๓.๑ นโยบายธรรมาภิบาลข้อมูล (Data Governance Policy) เพื่อให้ผู้เกี่ยวข้องกับข้อมูลทุกส่วนมั่นใจได้ว่าข้อมูลจะถูกใช้และจัดการได้อย่างสอดคล้องกับกรอบธรรมาภิบาลข้อมูลภาครัฐ มั่นคง ปลอดภัย และเป็นไปตามระเบียบ ข้อบังคับต่าง ๆ ของมหาวิทยาลัยสงขลานครินทร์

๓.๑.๑ กำหนดให้มีคณะกรรมการธรรมาภิบาลข้อมูล แต่งตั้งคณะบริกรข้อมูล และกำหนดบทบาทหน้าที่ความรับผิดชอบในการบริหารจัดการข้อมูล

๓.๑.๒ กำหนดหน่วยงานที่เป็นผู้ถือข้อมูลในการบริหารจัดการข้อมูล ในแต่ละชุดข้อมูล

๓.๑.๓ กำหนดมาตรฐานข้อมูล (Data Standard) และระเบียบปฏิบัติมาตรฐานและการบริหารจัดการคำอธิบายชุดข้อมูล (Metadata) ครอบคลุม บทบาทหน้าที่ความรับผิดชอบ กระบวนการจัดทำคำอธิบายชุดข้อมูลการควบคุมดูแลและสอบทานคำอธิบายชุดข้อมูล

๓.๑.๔ กำหนดคำนิยามข้อมูล (Data Definition) ขอบเขตและลักษณะข้อมูล (Scope of Data) และรูปแบบข้อมูล (Format of Data) ที่ครอบคลุมข้อมูลขนาดใหญ่ (Big data) และชุดข้อมูล

๓.๑.๕ จัดทำนโยบายธรรมาภิบาลข้อมูลที่ประกอบไปด้วย นโยบายคุณภาพข้อมูล (Data Quality Policy) นโยบายการเชื่อมโยงและการแบ่งปันข้อมูล (Data Transfer and Sharing Policy) นโยบายการจัดชั้นความลับข้อมูล (Data Classification Policy) นโยบายความเป็นส่วนบุคคลและความปลอดภัยของข้อมูล (Data Privacy and Security Policy) และนโยบายการเปิดเผยข้อมูล (Data Disclosure Policy)

๓.๑.๖ จัดทำธรรมาภิบาลข้อมูลตลอดวงจรชีวิตของข้อมูล (Data Lifecycle) ซึ่งประกอบด้วย กระบวนการสร้างข้อมูล (Data Creation) การจัดเก็บข้อมูล (Data Storage) การใช้ข้อมูล (Data Usage) การเผยแพร่ข้อมูล (Data Dissemination) การจัดเก็บข้อมูลถาวร (Data Archival) และการทำลายข้อมูล (Data Destruction)

๓.๑.๗ จัดให้มีกระบวนการในการบริหารจัดการความเสี่ยงด้านข้อมูล และสอดคล้องตามการบริหารความเสี่ยงของหน่วยงานเพื่อให้มีการบริหารจัดการข้อมูลที่ดี สอดคล้องกับระดับชั้นความลับและความพร้อมใช้

๓.๑.๘ กำหนดให้มีการสื่อสารและเผยแพร่นโยบายข้อมูลให้กับผู้ที่เกี่ยวข้องทั้งหน่วยงานภายในและภายนอก

๓.๑.๙ จัดให้มีการฝึกอบรม การสื่อสารเผยแพร่ เพื่อสร้างความตระหนักถึงธรรมาภิบาลข้อมูลและการบริหารจัดการข้อมูล โดยให้ครอบคลุมการบริหารจัดการทุกกระบวนการวงจรชีวิตของข้อมูล

๓.๑.๑๐ จัดให้มีการประเมินผลการดำเนินงาน ทบทวน ตรวจสอบ และปรับปรุงนโยบายอย่างต่อเนื่องอย่างน้อยปีละ ๑ ครั้ง

๓.๒ นโยบายคุณภาพข้อมูล (Data Quality Policy) เพื่อให้มีการควบคุมคุณภาพข้อมูลตลอดทั้งวงจรชีวิตของข้อมูล (Data Lifecycle) สำหรับการนำไปใช้ประโยชน์สูงสุดตามบริบทของข้อมูลอย่างเหมาะสม ในการบริหารข้อมูลและการให้บริการที่เกี่ยวกับข้อมูลของมหาวิทยาลัยสงขลานครินทร์ให้เป็นไปตามอำนาจหน้าที่ และวัตถุประสงค์ของมหาวิทยาลัยสงขลานครินทร์ โดยสอดคล้องตามระเบียบ หลักเกณฑ์ ของมหาวิทยาลัยและตามที่กฎหมายกำหนด

๓.๒.๑ กำหนดมาตรฐานข้อมูลให้เหมาะสมตามบริบทของข้อมูล และมีการควบคุมคุณภาพข้อมูลในการสร้าง การจัดเก็บ การใช้ การเผยแพร่ การจัดเก็บรักษา และการทำลายข้อมูล

๓.๒.๒ กำหนดให้มีข้อกำหนดพื้นฐานของการบริหารจัดการคุณภาพข้อมูล (Data Quality Management) โดยข้อมูลทุกชุดต้องมีคุณภาพข้อมูล (Data Quality) และมีความน่าเชื่อถือของข้อมูล (Data Integrity) รวมถึงแนวทางการควบคุมและการปรับปรุงอย่างต่อเนื่อง

๓.๒.๓ กำหนดให้มีการวัดคุณภาพข้อมูลและรายงานผลอย่างสม่ำเสมอตามบริบทของข้อมูล

๓.๒.๔ จัดอบรม ประชาสัมพันธ์เพื่อให้ผู้เกี่ยวข้องตระหนักถึงมาตรฐานข้อมูลและมีความเข้าใจถึงวิธีปฏิบัติในการควบคุมคุณภาพข้อมูลตลอดทั้งวงจรชีวิตข้อมูล (Data Lifecycle)

๓.๓ นโยบายการเชื่อมโยงและการแบ่งปันข้อมูล (Data Transfer and Sharing Policy) เพื่อให้มีการใช้ประโยชน์จากการเชื่อมโยง และการแบ่งปันข้อมูลระหว่างหน่วยงานที่เกี่ยวข้องทั้งภายในและภายนอก มีความมั่นคงปลอดภัยและข้อมูลมีคุณภาพ สามารถนำไปใช้ประโยชน์ได้อย่างมีประสิทธิภาพ ซึ่งสอดคล้องกับระเบียบ หลักเกณฑ์ และกฎหมายที่กำหนด บนพื้นฐานของประโยชน์ส่วนรวมเป็นสำคัญ

๓.๓.๑ กำหนดแนวปฏิบัติในการจัดการเรื่องความมั่นคงปลอดภัยในการเชื่อมโยงและการแบ่งปันข้อมูล โดยสามารถตรวจสอบย้อนกลับได้

๓.๓.๒ กำหนดกระบวนการในการเชื่อมโยง และการแบ่งปันข้อมูลให้ชัดเจน เริ่มตั้งแต่ขั้นตอนการเตรียมการ ขั้นตอนเริ่มดำเนินการ ขั้นตอนระหว่างดำเนินการ และขั้นตอนสิ้นสุดการดำเนินการ

๓.๓.๓ ดำเนินการตามสัญญาอนุญาต ข้อตกลงหรือหนังสือที่เป็นลายลักษณ์อักษรในการเชื่อมโยง และการแบ่งปันข้อมูล

๓.๓.๔ กำหนดเทคโนโลยีและมาตรฐานทั้งเชิงนโยบายและเชิงเทคนิคที่ใช้ในการเชื่อมโยง การร้องขอ และการแบ่งปันข้อมูล

๓.๔ นโยบายการจัดชั้นความลับข้อมูล (Data Classification Policy) เพื่อให้เกิดความชัดเจน ในการระบุถึงสิทธิ์ในการเข้าถึงและการใช้ประโยชน์จากข้อมูลได้อย่างถูกต้องตรงตามวัตถุประสงค์ โดยไม่ขัดต่อระเบียบ หลักเกณฑ์ และกฎหมาย

๓.๔.๑ ทุกชุดข้อมูลต้องมี การกำหนดชั้นความลับของข้อมูล การจัดเก็บในรูปแบบตามชั้นความลับของข้อมูลและการกำหนดสิทธิ์ในการเข้าถึงข้อมูล

๓.๔.๒ กำหนดแนวปฏิบัติและมาตรฐานของการเข้าถึงและการใช้งานตามชั้นความลับของข้อมูล

๓.๔.๓ ต้องมีการทบทวนระดับชั้นความลับข้อมูลและสิทธิ์ในการเข้าถึงข้อมูลอย่างน้อยปีละ ๑ ครั้ง และให้ดำเนินการปรับปรุงแนวปฏิบัติอย่างต่อเนื่อง

๓.๕ นโยบายความเป็นส่วนบุคคลและความปลอดภัยของข้อมูล (Data Privacy and Security Policy) เพื่อให้ข้อมูลทุกชุดข้อมูลถูกจัดเก็บรักษาอย่างปลอดภัย และป้องกันไม่ให้เกิดการเข้าถึงใช้งานหรือการเปิดเผยโดยไม่ได้รับอนุญาตให้เป็นไปตามกฎหมายว่าด้วยการรักษาความมั่นคงปลอดภัยทางไซเบอร์ และสำหรับข้อมูลส่วนบุคคลให้เป็นไปตามกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล และกฎหมายลำดับรองที่เกี่ยวข้อง

๓.๕.๑ กำหนดแนวปฏิบัติและมาตรฐานของในการสร้าง การจัดเก็บ การใช้ การเผยแพร่ การจัดเก็บรักษา และการทำลายข้อมูล โดยให้มีการตรวจสอบ และการประเมินผลเพื่อให้ตรวจสอบย้อนกลับได้

๓.๕.๒ จัดทำสถาปัตยกรรมความมั่นคงปลอดภัยของข้อมูล (Data Security and Privacy Architecture)

๓.๖ นโยบายการเปิดเผยข้อมูล (Data Disclosure Policy) เพื่อให้การเปิดเผยข้อมูลที่สามารถนำไปใช้ได้โดยอิสระ ส่งเสริมให้เกิดการนำไปใช้ประโยชน์ได้อย่างถูกต้อง ครบถ้วน โปร่งใส เท่าเทียมกันโดยไม่ขัดต่อกฎหมาย ระเบียบ และหลักเกณฑ์ที่เกี่ยวข้อง

๓.๖.๑ ห้ามเปิดเผยข้อมูลที่ขัดต่อกฎหมาย ระเบียบ และหลักเกณฑ์ ไม่ว่าข้อมูลจะอยู่ในรูปแบบใดหรือสถานที่ใดก็ตาม

๓.๖.๒ ให้มีการจัดเตรียมข้อมูลที่อยู่ในรูปแบบที่ได้จัดทำไว้เป็นมาตรฐานตามกำหนดและง่ายต่อการนำไปใช้

๓.๖.๓ ผู้ถือข้อมูลกับหน่วยงานที่เกี่ยวข้องต้องร่วมกันพิจารณาคัดเลือกชุดข้อมูลที่ต้องการเปิดเผย ให้เป็นไปตามแนวปฏิบัติที่ได้กำหนดไว้

๓.๖.๔ กำหนดแนวปฏิบัติและมาตรฐานของการสร้าง การจัดเก็บ การใช้ การเผยแพร่ การจัดเก็บรักษา และการทำลายข้อมูล โดยให้มีการตรวจสอบ และการประเมินผลเพื่อให้ตรวจสอบย้อนกลับได้

ข้อ ๔ เพื่อให้บรรลุวัตถุประสงค์และเป้าหมายที่สอดคล้องกับนโยบายธรรมาภิบาลข้อมูล (Data Governance Policy) มหาวิทยาลัยสงขลานครินทร์ฉบับนี้ได้อย่างเป็นรูปธรรม และเกิดประสิทธิผล ให้คณะกรรมการธรรมาภิบาลข้อมูลและคณะบริกรข้อมูล ติดตามและเฝ้าระวังกำกับดูแลข้อมูล รวมทั้งแนวโน้มความเสี่ยงใหม่ที่อาจจะเกิดขึ้น

ข้อ ๕ ส่วนงานภายในมหาวิทยาลัยที่ให้บริการระบบสารสนเทศอาจจะกำหนดแนวปฏิบัติการรักษาเพิ่มเติมเองได้ ทั้งนี้ต้องสอดคล้องกับนโยบายฉบับนี้

ข้อ ๖ ให้อธิการบดีรักษาการตามประกาศนี้ กรณีที่มีปัญหาเกี่ยวกับการบังคับใช้หรือการปฏิบัติตามประกาศนี้ ให้อธิการบดีมีอำนาจตีความและวินิจฉัยชี้ขาด และให้ถือเป็นที่สุด

ประกาศ ณ วันที่ ๒๖ สิงหาคม ๒๕๖๗

Digitally signed: 2024.08.27 14:26:31 +07:00

(ผู้ช่วยศาสตราจารย์ ดร.นิวัติ แก้วประดับ)

อธิการบดี