สถาบันมาตรวิทยาแห่งชาติ
National Institute of Metrology (Thailand)
NIMT

ประกาศสถาบันมาตรวิทยาแห่งชาติ
นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ พ.ศ. ๒๕๖๖

เพื่อให้การดำเนินงานด้านข้อมูลอิเล็กทรอนิกส์ผ่านระบบสารสนเทศของสถาบันมาตรวิทยาแห่งชาติเป็นไปอย่างมีประสิทธิภาพ มีความมั่นคง น่าเชื่อถือ และสอดคล้องกับพระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ. ๒๕๔๙ มาตรา ๕ และมาตรา ๗ ที่กำหนดให้หน่วยงานของรัฐต้องจัดทำนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศเพื่อให้การดำเนินการใดๆ ด้วยวิธีการทางอิเล็กทรอนิกส์กับหน่วยงานของรัฐหรือโดยหน่วยงานของรัฐมีความมั่นคงปลอดภัยและเชื่อถือได้ สถาบันมาตรวิทยาแห่งชาติจึงออกประกาศ ดังต่อไปนี้

ข้อ ๑ ประกาศนี้เรียกว่า "ประกาศสถาบันมาตรวิทยาแห่งชาติ เรื่องนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ"

ข้อ ๒ ประกาศนี้ให้ใช้บังคับตั้งแต่วันถัดจากวันประกาศเป็นต้นไป

ข้อ ๓ ในประกาศนี้

"สถาบัน" หมายความว่า สถาบันมาตรวิทยาแห่งชาติ

"ผู้ใช้งาน" หมายความว่าพนักงานลูกจ้างผู้ดูแลระบบผู้บริหารของสถาบันและบุคคลภายนอกที่ได้รับอนุญาตให้เข้าถึงและใช้งานระบบสารสนเทศของสถาบัน ได้ตามสิทธิที่ได้รับ

"ผู้ดูแลระบบ" หมายความว่าผู้ที่มีหน้าที่รับผิดชอบในการติดตาม ตรวจสอบ เฝ้าระวัง ดูแล บำรุงรักษา และบริหารจัดการระบบงาน ฐานข้อมูล ระบบคอมพิวเตอร์ ระบบเครือข่ายคอมพิวเตอร์

"ข้อมูล" หมายความว่าข้อความคำสั่งชุดคำสั่งหรือสิ่งอื่นใดบรรดาที่อยู่ในระบบคอมพิวเตอร์ในสภาพที่ระบบคอมพิวเตอร์สร้าง ส่ง รับ เก็บรักษา หรือประมวลผลได้ด้วยวิธีการทางอิเล็กทรอนิกส์บนอุปกรณ์

กระทรวงการอุดมศึกษา วิทยาศาสตร์ วิจัยและนวัตกรรม 3/4-5 หมู่ 3 ตำบลคลองห้า อำเภอคลองหลวง จังหวัดปทุมธานี 12120 โทรศัพท์ 0 2577 5100 โทรสาร 0 2577 3658
Ministry of Higher Education, Science, Research and Innovation 3/4-5 Mu 3, Khlong Ha, Khlong Luang, Pathum Thani 12120, Thailand. Tel. 0 2577 5100 Fax 0 2577 3658 www.nimt.or.th

สารสนเทศ หมายความว่า ข้อเท็จจริงที่ได้จากข้อมูลนำมาผ่านการประมวลผลการจัดระเบียบให้ข้อมูลซึ่งอาจอยู่ในรูปตัวเลข ข้อความ หรือภาพกราฟิก ให้เป็นระบบที่ผู้ใช้สามารถเข้าใจได้ง่ายและสามารถ

นำไปใช้ประโยชน์ในการบริหาร การวางแผน การตัดสินใจ และอื่นๆ

"ระบบคอมพิวเตอร์" หมายความว่าอุปกรณ์หรือชุดอุปกรณ์ของคอมพิวเตอร์ที่เชื่อมการทำงานเข้าด้วยกันโดยได้มีการกำหนดคำสั่งชุดคำสั่งหรือสิ่งอื่นใดและแนวทางปฏิบัติงานให้อุปกรณ์หรือชุดอุปกรณ์ ทำหน้าที่ประมวลผลข้อมูลโดยอัตโนมัติ

"ระบบเครือข่ายคอมพิวเตอร์" หมายความว่ากลุ่มของคอมพิวเตอร์และอุปกรณ์ต่างๆที่นำมาเชื่อมต่อกันเพื่อให้ผู้ใช้ในเครือข่ายสามารถติดต่อสื่อสาร แลกเปลี่ยนข้อมูล และใช้อุปกรณ์ต่างๆ ในเครือข่ายเดียวกันได้

"ระบบสารสนเทศ" หมายความว่าระบบที่นำเอาเทคโนโลยีสารสนเทศ ระบบคอมพิวเตอร์ และระบบเครือข่ายคอมพิวเตอร์ ชุดคำสั่งโปรแกรมคอมพิวเตอร์ มาช่วยในการสร้างสารสนเทศที่สถาบันสามารถนำมาใช้ประโยชน์ในการวางแผน บริหาร การสนับสนุนการให้บริหาร การพัฒนาและควบคุมการติดต่อสื่อสาร

"บัญชีผู้ใช้งาน" หมายความว่าบัญชีรายชื่อผู้เข้าถึงและใช้งานระบบสารสนเทศระบบคอมพิวเตอร์ และระบบเครือข่ายคอมพิวเตอร์ของสถาบัน

"สิทธิของผู้ใช้งาน" หมายความว่าสิทธิทั่วไป สิทธิจำเพาะ สิทธิพิเศษ และสิทธิอื่นใด ที่เกี่ยวข้องกับระบบสารสนเทศของสถาบัน

"สินทรัพย์" หมายความว่า สิ่งใดก็ตามที่มีคุณค่าสำหรับองค์กร เช่น เครื่องคอมพิวเตอร์และอุปกรณ์ เครื่องพิมพ์ เครื่องสแกนเนอร์ อุปกรณ์เครือข่ายคอมพิวเตอร์ สื่อบันทึกข้อมูล และโปรแกรมคอมพิวเตอร์ เป็นต้น

"การเข้าถึงหรือควบคุมการใช้งานสารสนเทศ" หมายความว่าการอนุญาตการกำหนดสิทธิหรือการมอบอำนาจให้ผู้ใช้งานเข้าถึงหรือใช้งานเครือข่ายหรือระบบสารสนเทศของสถาบันทั้งทางอิเล็กทรอนิกส์และทางกายภาพรวมทั้งการอนุญาตเช่นว่านั้นสำหรับบุคคลภายนอก

"ความมั่นคงปลอดภัยด้านสารสนเทศ" หมายความว่าการป้องกันข้อมูลในบริบทของ การรักษาความลับบูรณาภาพ และความพร้อมใช้งานของข้อมูลสถาบัน

"เหตุการณ์ด้านความมั่นคงปลอดภัย" หมายความว่า การเกิดเหตุการณ์ สภาพของบริการหรือเครือข่ายที่แสดงให้เห็นความเป็นไปได้ที่จะเกิดการฝ่าฝืนนโยบายด้านความมั่นคงปลอดภัยหรือมาตรการป้องกันที่ล้มเหลว หรือเหตุการณ์อันไม่อาจรู้ได้ว่าอาจเกี่ยวข้องกับความมั่นคงปลอดภัย

"สถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด" หมายความว่าสถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิดซึ่งอาจทำให้ระบบสารสนเทศ ระบบ

คอมพิวเตอร์ ระบบเครือข่ายคอมพิวเตอร์ ของสถาบันถูกบุกรุกหรือโจมตีและความมั่นคงปลอดภัยถูกคุกคาม

"พื้นที่ใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสาร" หมายความว่าพื้นที่ที่สถาบัน อนุญาตให้มีการใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสาร

"การประเมินความเสี่ยง" หมายความว่า การตรวจสอบโอกาสของผลลัพธ์ใดๆ ที่ไม่พึงประสงค์ต่อระบบสารสนเทศของสถาบัน และผลเสียที่อาจเกิดขึ้นตามมาได้

"การรักษาความครบถ้วน" หมายความว่า การรักษาข้อมูลคอมพิวเตอร์ กรอกข้อมูลอิเล็กทรอนิกส์ไว้ในสภาพสมบูรณ์ ขณะที่มีการใช้งาน การประมวลผล การโอนหรือการเก็บรักษา ไม่ให้มีการแก้ไขเปลี่ยนแปลง หรือทำลาย สารสนเทศโดยไม่ได้รับอนุญาตหรือโดยไม่ชอบ

"การรักษาความลับ" หมายความว่า การรักษาหรือสงวนไว้ซึ่งสิทธิในการเข้าถึงระบบสารสนเทศหรือระบบคอมพิวเตอร์ของบุคคลซึ่งได้รับอนุญาตเท่านั้น

"การรักษาสภาพพร้อมใช้" หมายความว่า การจัดทำให้ระบบสารสนเทศหรือระบบคอมพิวเตอร์นั้น สามารถทำงาน ใช้งานหรือเข้าถึงได้ในเวลาที่ต้องการ

"การรักษาความมั่นคงปลอดภัยทางกายภาพ" หมายความว่า มาตรการ นโยบาย หลักเกณฑ์ และกระบวนการใดๆ ที่ใช้ในการปกป้องทรัพยากรสารสนเทศ และสิ่งที่ปลูกสร้างหรืออุปกรณ์อื่นใดจากภัยคุกคามทางกายภาพที่อาจเกิดจากภัยธรรมชาติหรือและการคุกคามโดยผู้ไม่มีสิทธิ

ข้อ ๔ นโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

เพื่อให้การดำเนินงานด้านความมั่นคงปลอดภัยระบบสารสนเทศของสถาบันเป็นไปตามกฎหมายระเบียบปฏิบัติที่เกี่ยวข้อง รวมถึงเป็นแนวทางปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศอย่างเป็นลายลักษณ์อักษร ที่ได้รับการอนุมัติ และประกาศ เผยแพร่ให้ผู้ใช้งานและบุคคลที่เกี่ยวข้องรับทราบและถือปฏิบัติรวมทั้งมีการทบทวน ปรับปรุงนโยบายสม่ำเสมอ โดยมีรายละเอียดดังนี้

๔.๑ การเข้าถึงหรือควบคุมการใช้งานสารสนเทศ ครอบคลุมดังนี้ การเข้าถึงระบบสารสนเทศ การเข้าถึงระบบเครือข่าย การเข้าถึงระบบปฏิบัติการ และการเข้าถึงโปรแกรมประยุกต์หรือแอปพลิเคชัน

๔.๒ จัดให้มีระบบสารสนเทศและระบบสำรองของสารสนเทศ เพื่อให้มีความพร้อมใช้งานตลอดเวลาตามภารกิจของสถาบัน โดยมีการจัดทำแผนการเตรียมความพร้อมกรณีมีเหตุฉุกเฉิน เพื่อให้สามารถใช้งานสารสนเทศได้ตามปกติอย่างต่อเนื่อง

๔.๓ การตรวจสอบและประเมินความเสี่ยงด้านความมั่นคงปลอดภัยระบบสารสนเทศ อย่างน้อยปีละ๑ ครั้ง เพื่อนำมาปรับปรุงระบบให้มีความมั่นคงปลอดภัยยิ่งขึ้น

๔.๔ การอบรมเพื่อสร้างความรู้ความเข้าใจแก่ผู้ใช้งานระบบสารสนเทศเป็นไปอย่างถูกต้องเหมาะสม และปลอดภัย

ข้อ ๕ แนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

เพื่อให้ระบบสารสนเทศของสถาบัน มีความมั่นคงปลอดภัย น่าเชื่อถือ สอดคล้องกับนโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ จึงได้กำหนดแนวทางปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของสถาบัน ตามเอกสารแนบท้ายประกาศนี้ โดยให้มีการทบทวน ปรับปรุงตามความเหมาะสมอย่างน้อยปี ละ ๑ ครั้ง

ข้อ ๖ กลุ่มงานเทคโนโลยีสารสนเทศ เป็นผู้ดำเนินการทบทวน ปรับปรุงนโยบายและแนวปฏิบัติในประกาศนี้ตามความเหมาะสม อย่างน้อยปีละ ๑ ครั้ง

ประกาศ ณ วันที่ ๑๗ มิถุนายน พ.ศ. ๒๕๖๕

(นางอัจฉรา เจริญสุข)

ผู้อำนวยการสถาบันมาตรวิทยาแห่งชาติ

๑๗ มิ.ย. ๖๕ เวลา ๑๐:๕๒:๕๔ Non-PKI Server Sign

Signature Code : RgBBA-EEAMQ-BBADY-ARABC