ประกาศสำนักงานพัฒนาวิทยาศาสตร์และเทคโนโลยีแห่งชาติ
เรื่อง นโยบายการรักษาความมั่นคงปลอดภัยเว็บไซต์
ของสำนักงานพัฒนาวิทยาศาสตร์และเทคโนโลยีแห่งชาติ

เพื่อให้เว็บไซต์ภายใต้การควบคุมดูแลของสำนักงานพัฒนาวิทยาศาสตร์และเทคโนโลยีแห่งชาติ ซึ่งเป็นหน่วยงานของรัฐตามพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ สอดคล้องกับมาตรฐานการรักษาความมั่นคงปลอดภัยสำหรับเว็บไซต์ ตามประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง มาตรฐานการรักษาความมั่นคงปลอดภัยสำหรับเว็บไซต์ พ.ศ. ๒๕๖๘ ประกาศ ณ วันที่ ๑๐ กันยายน พ.ศ. ๒๕๖๘

อาศัยอำนาจตามความในมาตรา ๑๕ แห่งพระราชบัญญัติพัฒนาวิทยาศาสตร์และเทคโนโลยี พ.ศ. ๒๕๓๔ จึงกำหนดนโยบายการรักษาความมั่นคงปลอดภัยเว็บไซต์ของสำนักงานพัฒนาวิทยาศาสตร์และเทคโนโลยีแห่งชาติไว้ดังนี้

๑. หลักการ

สำนักงานพัฒนาวิทยาศาสตร์และเทคโนโลยีแห่งชาติจัดให้มีข้อกำหนดสำหรับการใช้งาน การดูแลรักษาและการป้องกันที่เหมาะสมกับลักษณะการดำเนินกิจการของสำนักงาน ซึ่งการดูแลรักษาและการป้องกันมุ่งหมายเพื่อรักษาความมั่นคงปลอดภัย โดยมีหลักการสำคัญคือการธำรงไว้ซึ่งการรักษาความลับ การรักษาความถูกต้องครบถ้วน และการรักษาสภาพพร้อมใช้งาน ดังนี้

(๑) <u>การรักษาความลับ (Confidentiality)</u> หมายถึง การป้องกันไม่ให้ทรัพย์สินสามารถถูกเข้าถึงได้จากผู้ไม่มีสิทธิ โดยการเข้าถึงนั้นรวมถึงการถูกเปิดเผยและการจำแนกแจกจ่ายซึ่งทรัพย์สินนั้นด้วย ดังนั้น ในการรักษาความลับจึงต้องมีมาตรการควบคุมทั้งทางกายภาพและทางเทคนิค โดยผู้ไม่มีสิทธิจะต้องไม่สามารถเข้าถึงทรัพย์สินนั้นได้ รวมทั้งการจำแนกทรัพย์สิน และการกำหนดระดับความต้องการในการป้องกันไว้อย่างชัดเจน เพื่อให้ผู้ถือครองทรัพย์สินปฏิบัติได้ถูกต้องเหมาะสมกับระดับความต้องการนั้น

(๒) <u>การรักษาความถูกต้องครบถ้วน (Integrity)</u> หมายถึง การป้องกันไม่ให้ทรัพย์สินถูกเปลี่ยนแปลงแก้ไขทั้งโดยเจตนาหรือไม่เจตนาจากผู้ไม่มีสิทธิที่จะแก้ไขทรัพย์สินนั้น ดังนั้น การควบคุมและป้องกันจึงต้องประกอบด้วยการกำหนดสิทธิในการแก้ไข การกำหนดสิทธิในการเข้าถึง และจำเป็นต้องอาศัยการตรวจสอบทั้งจากการทำรายการบัญชีทรัพย์สินและทางเทคนิคประกอบด้วย

(๓) <u>การรักษาสภาพพร้อมใช้งาน (Availability)</u> หมายถึง การที่ผู้มีสิทธิสามารถเข้าใช้งานทรัพย์สินได้เมื่อต้องการใช้งานทั้งทางกายภาพและทางเทคโนโลยี เช่น การให้บริการระบบจดหมายอิเล็กทรอนิกส์ที่จำเป็นจะต้องให้บริการตลอดเวลา ดังนั้น เมื่อผู้ใช้ต้องการจะรับหรือส่งจดหมายอิเล็กทรอนิกส์ ระบบจำเป็นที่จะต้องสามารถให้บริการได้ตลอดเวลาเป็นต้น

๒. นโยบายการปฏิบัติ

๒.๑ จัดให้มีการประเมินความเสี่ยงอย่างน้อยปีละ ๑ ครั้ง และทุกครั้งที่มีการเปลี่ยนแปลงอย่างมีนัยสำคัญ โดยจะพิจารณาถึงบริบทภายใน (Internal Context) บริบทภายนอก (External Context) ผู้ที่มีส่วนได้ส่วนเสีย (Interested Party) วิสัยทัศน์ พันธกิจ การเปลี่ยนแปลงของระบบความมั่นคงปลอดภัยไซเบอร์ ความเสี่ยง และมาตรฐานสากล อย่างมีนัยสำคัญ

๒.๒ มีการกำหนด...

๒.๒ มีการกำหนดเกณฑ์ความเสี่ยงที่ยอมรับได้และความเสี่ยงที่ยอมรับไม่ได้ เพื่อใช้เป็นแนวทางในการบริหารจัดการความเสี่ยงที่เกิดขึ้นในการประเมินความเสี่ยงที่เกิดขึ้น

๒.๓ จัดให้มีการทบทวนนโยบายอย่างน้อยปีละ ๑ ครั้ง หรือเมื่อมีการเปลี่ยนแปลงที่สำคัญ

๒.๔ มีการกำหนดแผนการรับมือภัยคุกคามทางไซเบอร์ เพื่อรับมือและตอบสนองต่อเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยทางไซเบอร์

๒.๕ มีการประเมินผลสัมฤทธิ์ของนโยบาย เพื่อนำมาปรับปรุงนโยบายให้สอดคล้องกับภัยคุกคามในปัจจุบันและภัยคุกคามที่อาจเกิดขึ้นได้ในอนาคต

๒.๖ จัดให้มีทรัพยากรด้านงบประมาณ ทรัพยากรบุคคล และการบริหารจัดการเทคโนโลยีที่เพียงพอต่อการบริหารจัดการด้านความมั่นคงปลอดภัยของสำนักงานพัฒนาวิทยาศาสตร์และเทคโนโลยีแห่งชาติ

๓. โครงสร้างทางด้านความมั่นคงปลอดภัยทางไซเบอร์

สำนักงานพัฒนาวิทยาศาสตร์และเทคโนโลยีแห่งชาติได้กำหนดมาตรการควบคุม กำกับและติดตามการปฏิบัติหน้าที่ด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์สำหรับส่วนงานต่าง ๆ ทั้งภายในและภายนอกองค์กร โดยมีวัตถุประสงค์เพื่อมุ่งเน้นการธำรงไว้ซึ่งการรักษาความลับ (Confidentiality) การรักษาความถูกต้องครบถ้วน (Integrity) และการรักษาสภาพพร้อมใช้งาน (Availability) ตามประกาศสำนักงานพัฒนาวิทยาศาสตร์และเทคโนโลยีแห่งชาติ เรื่อง นโยบาย ประมวลแนวทางปฏิบัติ และกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของสำนักงานพัฒนาวิทยาศาสตร์และเทคโนโลยีแห่งชาติ

๔. นโยบายความมั่นคงปลอดภัยที่เกี่ยวข้องกับทรัพยากรบุคคล

สำนักงานพัฒนาวิทยาศาสตร์และเทคโนโลยีแห่งชาติมีกระบวนการในการคัดเลือกบุคลากร การฝึกอบรมและควบคุมการปฏิบัติงานของบุคลากรอย่างเหมาะสมตลอดระยะเวลาการปฏิบัติงาน เพื่อให้บุคลากรของสำนักงานพัฒนาวิทยาศาสตร์และเทคโนโลยีแห่งชาติเข้าใจถึงหน้าที่และความรับผิดชอบของตนในการรักษาความมั่นคงปลอดภัยของข้อมูลและระบบสารสนเทศทั้งก่อนการเริ่มปฏิบัติงาน ระหว่างการปฏิบัติงาน การเปลี่ยนแปลงตำแหน่งงาน หรือเมื่อสิ้นสุดการปฏิบัติงานกับสำนักงานพัฒนาวิทยาศาสตร์และเทคโนโลยีแห่งชาติด้วย

๕. การบริหารจัดการทรัพย์สิน

สำนักงานพัฒนาวิทยาศาสตร์และเทคโนโลยีแห่งชาติกำหนดให้มีการระบุทรัพย์สินที่สำคัญและกำหนดหน้าที่ความรับผิดชอบอย่างเหมาะสมในการปกป้องทรัพย์สินจากภัยคุกคาม ช่องโหว่ ผู้บุกรุก การถูกโจรกรรม และสิ่งที่อาจสร้างความเสียหาย ซึ่งประกอบด้วย

(๑) นโยบายการจำแนกชั้นความลับสารสนเทศ (Information Classification Policy) เพื่อให้สารสนเทศได้รับการปกป้องที่เหมาะสมโดยสอดคล้องกับความสำคัญของสารสนเทศนั้น ๆ

(๒) ขั้นตอนการปฏิบัติงานการจัดการบัญชีทรัพย์สิน (Inventory of Assets Procedure) เพื่อระบุทรัพย์สินที่สำคัญของสำนักงานพัฒนาวิทยาศาสตร์และเทคโนโลยีแห่งชาติและประเมินความเสี่ยงของทรัพย์สินเหล่านั้น รวมถึงกำหนดหน้าที่ความรับผิดชอบในการปกป้องทรัพย์สินอย่างเหมาะสม

(๓) นโยบายการใช้งานข้อมูลและระบบเทคโนโลยีสารสนเทศ (IT Acceptable Usage Policy) เพื่อป้องกันการเปิดเผย การเปลี่ยนแปลงแก้ไข การลบหรือการทำลาย ทรัพย์สินสารสนเทศโดยไม่ได้รับอนุญาต

๖. การควบคุม...

๖. การควบคุมการเข้าถึง

สำนักงานพัฒนาวิทยาศาสตร์และเทคโนโลยีแห่งชาติมีนโยบายควบคุมการเข้าถึงระบบสารสนเทศเฉพาะผู้ที่ได้รับอนุญาต เพื่อป้องกันการเปิดเผยหรือการโจรกรรมสารสนเทศและอุปกรณ์สารสนเทศ สร้างความมั่นคงปลอดภัยให้กับการดำเนินงานของสำนักงานพัฒนาวิทยาศาสตร์และเทคโนโลยีแห่งชาติ ซึ่งประกอบด้วย

(๑) นโยบายการควบคุมการเข้าถึงระบบเทคโนโลยีสารสนเทศ (System Access Control Policy) เพื่อควบคุมการเข้าถึงโปรแกรมประยุกต์หรือแอปพลิเคชันและสารสนเทศ รักษาความมั่นคงปลอดภัยและป้องกันการเข้าถึงระบบสารสนเทศโดยไม่ได้รับอนุญาต

(๒) ขั้นตอนการปฏิบัติงานการขอเข้าถึงระบบ (Access Request Procedure) กำหนดสิทธิและควบคุมการเข้าถึงข้อมูลและการใช้งานระบบสารสนเทศ ปกป้องข้อมูลและสารสนเทศจากการเข้าถึงโดยผู้ที่ไม่ได้รับอนุญาต

๗. การเข้ารหัสลับข้อมูล

สำนักงานพัฒนาวิทยาศาสตร์และเทคโนโลยีแห่งชาติกำหนดขั้นตอนการปฏิบัติงานการเข้ารหัสลับข้อมูล (Cryptography Procedure) เพื่อรักษาไว้ซึ่งความลับของข้อมูล การพิสูจน์ตัวตนของผู้ใช้งานระบบสารสนเทศ และป้องกันการแก้ไขข้อมูลจากผู้ที่ไม่ได้รับอนุญาตอย่างมีประสิทธิภาพและเหมาะสม

๘. นโยบายความมั่นคงปลอดภัยทางด้านกายภาพและสิ่งแวดล้อม

สำนักงานพัฒนาวิทยาศาสตร์และเทคโนโลยีแห่งชาติกำหนดมาตรการการควบคุมและป้องกันและเป็นมาตรฐานความมั่นคงปลอดภัยที่เกี่ยวข้องกับการเข้าใช้งานหรือการเข้าถึงอาคาร สถานที่ พื้นที่ใช้งานระบบสารสนเทศ โดยพิจารณาตามความสำคัญของอุปกรณ์ระบบสารสนเทศ ข้อมูลซึ่งเป็นทรัพย์สินที่มีค่าและอาจจำเป็นต้องรักษาความลับ โดยมาตรการนี้จะมีผลบังคับกับทั้งบุคลากรของสำนักงานพัฒนาวิทยาศาสตร์และเทคโนโลยีแห่งชาติและผู้ให้บริการภายนอก

จึงประกาศเพื่อทราบและถือปฏิบัติโดยทั่วกัน

ประกาศ ณ วันที่ ๒๐ มีนาคม พ.ศ. ๒๕๖๙

(ศาสตราจารย์ชูกิจ ลิมปิจำนงค์)
ผู้อำนวยการ
สำนักงานพัฒนาวิทยาศาสตร์และเทคโนโลยีแห่งชาติ